UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

ROBERT L. BAX, derivatively on behalf of EQUIFAX, INC.,

Plaintiff,

v.

RICHARD F. SMITH, JOHN W. GAMBLE, JR., JOHN J. KELLEY, III, RODOLFO O. PLODER, JOSEPH M. LOUGHRAN, III, ROBERT D. DALEO, WALTER W. DRIVER, JR., MARK L. FEIDLER, G. THOMAS HOUGH, L. PHILLIP HUMANN, ROBERT D. MARCUS, SIRI S. MARSHALL, JOHN A. MCKINLEY, ELANE B. STOCK, and MARK B. TEMPLETON,

Defendants,

-and-

EQUIFAX, INC., a Georgia Corporation,

Nominal Defendant.

Case No.:

DEMAND FOR JURY TRIAL

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

TABLE OF CONTENTS

Page

By and through his undersigned counsel, Plaintiff Robert L. Bax ("Plaintiff") brings this shareholder derivative action on behalf of Nominal Defendant Equifax, Inc. ("Equifax" or the "Company") and against certain current and former officers and directors of the Company for breaches of fiduciary duties, unjust enrichment, insider selling, violation of Section 14(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), issuing false and misleading statements in violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5 promulgated thereunder, violations of Section 29(b) of the Exchange Act, corporate waste, and contribution and indemnification. Plaintiff makes these allegations upon personal knowledge as to those allegations concerning himself and, as to all other matters, upon the investigation of counsel, which includes, without limitation: (a) review and analysis of public filings made by Equifax and other related parties with the United States Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases and other publications disseminated by certain officers and directors of Equifax named as defendants herein (the "Individual Defendants" (further defined below in ¶37) and other related non-parties; (c) review of news articles, shareholder communications, and postings on Equifax's website concerning the Company's public statements; (d) pleadings, papers, and any documents filed with, and publicly available from, the many lawsuits filed against Equifax, including the related

pending securities fraud class actions,[1] the hundreds of pending consumer lawsuits filed nationwide,[2] and the pending consumer protection lawsuits filed by various states, cities, and other municipalities;[3] and (e) review of other publicly available information concerning Equifax and the Individual Defendants.

I. NATURE OF THE ACTION AND OVERVIEW

1. Between March 10, 2017 and May 13, 2017,[4] attacker(s) infiltrated Equifax's servers and gained unfettered access to the personally-identifiable

[1] On January 10, 2018, the pending securities class actions arising from the Equifax data breach (the "Data Breach") (the "Securities Class Actions") were consolidated and are styled, *In re Equifax Inc. Securities Litigation*, Consolidated Case No. 1:17-cv-03463-TWT (N.D. Ga.).

[2] Hundreds of consumer class action lawsuits were filed against Equifax arising from the Data Breach, which also include class action lawsuits filed on behalf of financial institutions alleging they were damaged by the Data Breach (collectively, the "Consumer Class Actions"), and these lawsuits have been consolidated into *In re: Equifax, Inc., Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT, MDL No. 2800 ("Consumer MDL"). On December 6, 2017, the JPML issued its Transfer Order and listed the cases to be included within the Consumer MDL. *See* Consumer MDL Dkt. No. 1.

[3] The consumer protection actions filed against Equifax (collectively, the "Consumer Protection Actions") include at least the following: *Commonwealth of Mass. v. Equifax, Inc.*, Case No. 1784-CV-03009 (Suffolk Cnty. Super. Ct.), filed Sept. 19, 2017; *People of the State of Cal. v. Equifax, Inc., et al.*, Case No. CGC-17-561529 (San Francisco Cnty. Super. Ct.), filed Sept. 26, 2017; and *City of Chicago v. Equifax, Inc.*, Case No. 1:17-cv-7798 (N.D. Ill.), filed Sept. 28, 2017.

[4] The Company initially reported, by press release dated September 15, 2017, that it "believe[d] the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017." However, data security

information ("PII") that Equifax maintained for approximately 145.5 million Americans, causing the Data Breach. Additionally, the hackers were able to continue accessing Equifax's servers and the consumer PII stored thereupon until July 30, 2017, and apparently without detection by Equifax until July 29, 2017. The PII that was compromised includes names, social security numbers ("SSNs"), birth dates, addresses, driver's license numbers, credit card information, and other critically sensitive information.

2. Through this derivative action, Plaintiff brings claims against the Individual Defendants and seeks to remedy the harm suffered by the Company and its shareholders in connection with the Data Breach, the most damaging and far-reaching compromise of consumer financial data in known history. Holding executives such as the Individual Defendants personally liable for the harm inflicted on the Company and its shareholders would incentivize others to enact adequate measures to protect PII going forward, including investing in staffing and technology

---

firm FireEye's Mandiant group ("Mandiant") said the first evidence of hackers' infiltration of the Company actually occurred on March 10, 2017, according to a confidential note reviewed by The Wall Street Journal that Equifax sent to some of its customers. *See* AnnaMaria Andriotis and Robert McMillan, *Hackers Entered Equifax Systems in March*, The Wall Street Journal, https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617 (last visited on Jan. 19, 2018).

sufficient to safeguard the critically sensitive information they've accepted responsibility for protecting.

3. The Individual Defendants named herein knowingly and completely failed to undertake their responsibilities by consciously failing to oversee their data security oversight systems and controls. Despite knowing these systems were inadequate at detecting, preventing, and resolving data breaches, the Individual Defendants demonstrated a complete disregard for securing the very sensitive consumer data that drives their core businesses. Indeed, PII ***is*** Equifax's business.

4. The Individual Defendants consciously failed to act in the face of a known duty to protect the critically confidential and sensitive PII of consumers, and consciously failed to present investors with accurate information regarding the Company's lack of even the most basic data security controls and systems. For example, the Company has admitted that the data compromised in Equifax's online disputes portal at issue was stored in unencrypted plaintext and would have been easily readable by attackers. Worse, the Company utterly failed to patch[5] an Apache Struts 2 vulnerability—involving the software that hackers exploited in the Data

[5] According to Professor Jamie Winterton, Director of Strategy at Arizona State University's Global Security Initiative, who testified before the U.S. Senate on October 4, 2017, regarding the Data Breach, "[p]atching isn't trivial, but it's possibly the most important piece of a company's security posture. . . . [Patching] should be well understood at the C-suite level."

Breach and the application that Equifax uses in its online disputes portal—***until after*** the Data Breach, despite, for example, (i) a March 8, 2017 alert from U.S. Computer Emergency Readiness Team ("US-CERT") warning Equifax of the dire need to do so; (ii) knowledge of a 2016 Deloitte security audit of Equifax's data security that specifically identified Equifax's careless approach to patching systems; and (iii) a warning from Mandiant, in March or April 2017, that Equifax's unpatched systems and misconfigured security policies could indicate major problems. As a result, the Company waited over four and a half months to fix a dangerous security flaw that should have been addressed on March 8, 2017, leading to disastrous consequences.

5. In fact, data breaches, such as the Data Breach, and the fraud and risk of fraud that follows for consumers, actually serve to benefit the Individual Defendants. Specifically, data breaches facilitate identify theft and other fraud, which, in turn, generates business for the Company by driving consumers and businesses to purchase Equifax's credit monitoring and credit locking services, which, in turn, increases the Individual Defendants' incentive-based compensation. On August 17, 2017, after learning of the Data Breach, Equifax's Chief Executive Officer ("CEO") at the time, Defendant Richard Smith ("Smith"), admitted during a speech before the University of Georgia's Terry College of Business (the "August 17

Terry College Speech")[6] that fraud was a "a huge opportunity for Equifax," and that fraud was a "massive, growing business" for the Company. Following the Data Breach, millions of consumers have signed up for Equifax's credit monitoring services, whether sold directly by Equifax or indirectly through other businesses such as LifeLock, Inc., a subsidiary of Symantec Corp. ("LifeLock"), which purchases and resells Equifax credit monitoring services to consumers. Many experts believe credit locking and monitoring programs are primarily methods credit bureaus such as Equifax use to establish contractual relationships with consumers to sidestep state law mandated "credit freeze" protections and, instead, impose terms and conditions favorable to credit bureaus.

6. Indeed, the Individual Defendants were more interested in furthering and protecting their own interests than those of consumers, the Company, or its shareholders. In fact, Defendants have, in effect, incentivized Equifax's lax data security by ***excluding the costs of legal settlements made by the Company*** when determining its top executives' incentive compensation.

7. During the two-month period that the Individual Defendants recklessly withheld disclosure of the Data Breach, the 145.5 million affected consumers were helpless to protect their PII. Not everyone was harmed by the delay, however. Four

[6] https://www.youtube.com/watch?v=lZzqUnQg-Us (last visited Jan. 10, 2018).

Equifax executives—Defendant John W. Gamble, Jr. ("Gamble") (Chief Financial Officer or "CFO"), Defendant Joseph M. Loughran, III ("Loughran") (President, U.S. Information Solutions), and Defendant Rodolfo O. Ploder ("Ploder") (President, Workforce Solutions) exploited their positions as corporate fiduciaries of Equifax and sold their personal stock holdings for millions of dollars in insider profits just days after the Company purportedly learned of the Data Breach.

8. As a result of the foregoing, Equifax's public statements, made or caused to be made by certain Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times. These Defendants caused Equifax to issue false and misleading statements concerning the Company's data security, business practices, operations, financials, compliance policies and practices, and internal controls. Specifically, these Defendants made, or caused the Company to make, false and/or misleading statements, and/or failed to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks

concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by harm they caused the Company; (vii) the Company had inadequate corporate financial-reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial reporting; (x) the Company was recklessly relying on a single employee to address US-CERT warnings regarding critical data security systems; (xi) the Company had been warned by Deloitte in 2016 that Equifax was taking a careless approach to patching critical data security systems; (xii) Mandiant, in March or April 2017, had warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems; (xiii) the Company lacked a plan to quickly, effectively, and sufficiently respond to a major data breach; and (xiv) as a result of the foregoing, Equifax's public statements, made or caused to be made by certain Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times.

9. Indeed, despite learning that its data security systems were not legally compliant, the Individual Defendants consciously failed to, *inter alia*: (i) develop, implement, and maintain basic measures to safeguard and protect its data systems; (ii) develop, implement, and maintain basic monitoring systems to detect security breaches; (iii) develop, implement, and maintain basic data security systems, controls, and monitoring systems; (iv) develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) adequately assess critical risks associated with the Company's data security; (vi) develop a plan to quickly, effectively, and sufficiently respond to a major data breach before the Data Breach occurred; (vii) adequately assess the risks associated with the Company's executive compensation plan and revise the executive compensation plan to make sure executives were held accountable for legal costs associated with corporate trauma caused by their action or inaction; (viii) maintain adequate corporate accounting and corporate financial-reporting resources; (ix) adequately assess the risks associated with the Company's financial reporting; and (x) maintain effective internal controls over financial reporting.

10. As a result of the Individual Defendants' conduct, the price of Equifax stock was artificially inflated during parts of the Relevant Period.[7]

11. When the market discovered the Data Breach and the true facts surrounding it, it reacted swiftly and severely to the news. Specifically, on September 8, 2017, the Company's stock price tumbled $19.49 per share (or approximately 13.7%), on unusually high trading volume, to close at $123.23 per share, resulting in a loss of approximately $2.34 billion in market capitalization. In the days that followed, the stock continued declining at a catastrophic rate, reaching a low of $92.98 per share at the close of trade on September 15, 2017 (eight days after the Data Breach was disclosed), representing a decline of $49.74 (or approximately 34.9%) per share, and a loss of approximately $6 billion in market capitalization, compared to the price at close of trade on September 7, 2017 (the last day of trading before disclosure of the Data Breach).

12. Worse still, the Individual Defendants grossly mismanaged the Company's response to the Data Breach. For example, Equifax concedes that it discovered the Data Breach on July 29, 2017, but nonetheless waited nearly six weeks to disclose the Breach to affected consumers and Equifax's shareholders.

[7] The Relevant Period begins on February 22, 2017, and continues through the present, as the harm to the Company is continuing.

After finally disclosing the Data Breach, Equifax "offered" one year of free credit monitoring to consumers affected by the Data Breach, but included in the terms of service of its Data Breach notification site, equifaxsecurity2017.com, an arbitration clause and class action waiver that barred those who enrolled in the Equifax credit monitoring program from participating in any class action lawsuits that may arise from the incident. Though the Company issued a statement, on the evening of September 8, 2017, noting that "[i]n response to consumer inquiries, we have made it clear that the arbitration clause and class action waiver included in the Equifax and TrustedID Premier terms of use does not apply to this cybersecurity incident" and later confirmed its removal from the terms of service of its Data Breach notification web site (on September 10, 2017), it did so only after facing a backlash of negative publicity and criticism from consumers and government regulators alike.

13. Before filing this action, pursuant to O.C.G.A. § 14-2-742, Plaintiff first demanded, by letter sent to the Board of Directors of Equifax (the "Board") on September 11, 2017 (the "Demand") (attached hereto as **Exhibit A**), that the Company's directors take suitable action. More than ninety days have expired from the date the Demand was made. Despite having months to investigate the wrongdoing described in the Demand, and despite the Company announcing on September 7, 2017, that "the Company's investigation is substantially complete,"

the Company has yet to take suitable legal action against any officer or director of the Company found to have committed or participated in the wrongdoing described in the Demand.

14. Nor can the Company plausibly require more time to investigate—the Board was able to investigate, and determine by report dated November 1, 2017, that certain Equifax insider-selling executives "traded appropriately" when selling stock just days after the Company learned of the Data Breach. The Court and the Company's shareholders cannot reasonably repose confidence in the Board to investigate this matter given this public and prematurely-issued finding exculpating Company insiders whose conduct is supposed to be impartially investigated by the Board, at a time when the Board's investigation was just getting underway.

15. Plaintiff now brings this suit derivatively on Equifax's behalf to (i) remedy the Individual Defendants' conscious failures to take reasonable action in the face of known threats to, and vulnerabilities in, its data security systems, controls, and monitoring systems, and (ii) seek redress for the Individual Defendants' breaches of fiduciary duties, unjust enrichment, insider selling, violation of Section 14(a) of the Exchange Act, issuing false and misleading statements in violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5

promulgated thereunder, violations of Section 29(b) of the Exchange Act, and corporate waste.

II. JURISDICTION AND VENUE

16. The Court has jurisdiction over all claims under 28 U.S.C. § 1331 in that the Complaint states a federal question. The Court has supplemental jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a). The Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(2) because (i) complete diversity exists between Plaintiff and each Defendant, and (ii) the amount in controversy exceeds $75,000. This action is not a collusive action designed to confer jurisdiction on a court of the United States that it would not otherwise have.

17. The Court has personal jurisdiction over each Defendant because each Defendant is either a corporation that does sufficient business in Georgia, or is an individual who has sufficient minimum contacts with Georgia, so as to render the exercise of jurisdiction by the Georgia courts permissible under traditional notions of fair play and substantial justice.

18. Venue is proper in this District under 28 U.S.C. § 1391 because: (a) Equifax maintains its principal executive offices in this District; (b) one or more of the Defendants reside in this District; (c) a substantial portion of the transactions

and wrongs complained of herein—including the Individual Defendants' primary participation in the wrongful acts—occurred in this District; and (d) the Individual Defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

19. In connection with the acts and conduct alleged herein, Defendants, directly and indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the United States mails, interstate telephone communications, and the facilities of the national securities exchanges and markets.

III. PARTIES

20. Plaintiff Robert L. Bax has been an Equifax shareholder since 2005 and is, and at all relevant times has been, a holder of Equifax common shares.

21. Nominal Defendant Equifax was founded in 1899, and is the oldest of the three major U.S. credit reporting agencies. The Company began as an investigation firm that gathered data on customers paying their bills so that grocers could know which customers were creditworthy. The Company went public in January 1978, and its common stock is traded on the New York Stock Exchange ("NYSE") under the ticker symbol "EFX," with approximately 120.08 million shares outstanding. Equifax is incorporated in Georgia, and also maintains its

principal executive offices in Georgia, located at 1550 Peachtree Street NW, Atlanta, Georgia 30309.

22. Defendant Smith served as a director of the Company, beginning September 22, 2005, and as the Company's Chairman of the Board and CEO, beginning December 15, 2005, until he retired from all positions effective September 26, 2017. Smith received a sum of $41,766,949 in total compensation from Equifax from 2014 to 2016, including $13,879,675 in 2014, $12,922,711 in 2015, and $14,964,563 in 2016. Additionally, in connection with his retirement, Smith became entitled to and/or received a pension payout of approximately $18.3 million. While in possession of material, non-public information, Smith sold at least 74,346 personally-held shares of Equifax stock, at artificially-inflated prices, for proceeds of $9,742,076.80. Smith is named as a defendant in each of the Securities Class Actions.

23. Defendant Gamble has served as the Company's CFO and Corporate Vice President since May 2014. Gamble received a sum of $13,227,853 in total compensation from Equifax from 2014 to 2016, including $7,079,102 in 2014, $3,053,644 in 2015, and $3,095,107 in 2016. While in possession of material, non-public information, Gamble sold at least 20,500 personally-held shares of Equifax stock (nearly 33% of his total holdings), at artificially-inflated prices, for proceeds

of approximately $2,856,506. Gamble is named as a defendant in each of the Securities Class Actions.

24. Defendant John J. Kelley, III ("Kelley") has served as Chief Legal Officer, Corporate Vice President, and Corporate Secretary since January 1, 2013. Kelley received a sum of $7,813,635 in total compensation from Equifax from 2014 to 2016, including $2,420,273 in 2014, $2,597,666 in 2015, and $2,795,696 in 2016. During the Relevant Period, while in possession of material, non-public information, Kelley sold at least 8,500 personally-held shares of Equifax stock (i.e., nearly 42% of his total holdings), at artificially-inflated prices, for proceeds of $1,112,200.35.

25. Defendant Ploder has served as the Company's President of Workforce Solutions since November 2015. Prior to leading Workforce Solutions, he led U.S. Information Solutions at Equifax and was responsible for all U.S.-based services that provide businesses with consumer and commercial information, specifically related to risk management, fraud, marketing, and other industry-specific areas. Ploder received a sum of $4,840,426 in total compensation from Equifax from 2015 to 2016, including $2,080,109 in 2015, and $2,760,317 in 2016. While in possession of material, non-public information, Ploder sold at least 1,719 personally-held shares of Equifax stock, at artificially-inflated prices, for proceeds of $250,458.30.

26. Defendant Loughran has served as the Company's President of U.S. Information Solutions since July 1, 2017. Prior to assuming that role, Loughran served in several key executive roles within Equifax, including as Chief Marketing Officer ("CMO") from March 31, 2015 until July 1, 2017, President of North America Personal Solutions (now Global Consumer Solutions) from January 4, 2010 until March 31, 2015, Senior Vice President of Corporate Development from April 2006 until December 2009, and Senior Vice President of Mergers and Acquisitions from March 2006 until April 2006. While in possession of material, non-public information, Loughran sold at least 7,604 personally-held shares of Equifax stock, at artificially-inflated prices, for proceeds of $1,056,804.49. On August 1, 2017, Loughran also exercised an option to purchase 3,000 shares at a price of $33.60 per share (a discount of $112.66 per share from the market price of Equifax stock at the close of trade on that date—i.e., a total discount of $337,980).

27. Defendant Robert D. Daleo ("Daleo") has served as a director of the Company since August 7, 2006. Daleo received a sum of $503,684 in total compensation from Equifax from 2015 to 2016, including $242,688 in 2015, and $260,996 in 2016. During the Relevant Period, Daleo served as Chair of the Audit Committee, and as a member of the Executive Committee, and the Compensation,

Human Resources & Management Succession Committee (the "Compensation Committee").

28. Defendant Walter W. Driver, Jr. ("Driver") has served as a director of the Company since November 8, 2007. Driver received a sum of $475,495 in total compensation from Equifax from 2015 to 2016, including $236,628 in 2015, and $238,867 in 2016. During the Relevant Period, Driver served as a member of the Governance Committee.

29. Defendant Mark L. Feidler ("Feidler") has served as a director of the Company since March 1, 2007, and has served as Chairman of the Board since September 26, 2017. Feidler received a sum of $495,100 in total compensation from Equifax from 2015 to 2016, including $239,128 in 2015, and $255,972 in 2016. During the Relevant Period, Feidler served as Chair of the Executive Committee, and as a member of the Governance Committee and the Technology Committee.

30. Defendant G. Thomas Hough ("Hough") has served as a director of the Company since October 1, 2016. Hough received a sum of $174,425 in total compensation from Equifax in 2016. During the Relevant Period, Hough served as a member of the Audit Committee and the Technology Committee. Hough has been named as a member of the Demand Review Committee formed by the Board in response to Plaintiff's Demand.

31. Defendant L. Phillip Humann ("Humann") has served as a director of the Company since 1992, and has served as "presiding director" since September 2008. Humann received a sum of $522,812 in total compensation from Equifax from 2015 to 2016, including $258,938 in 2015, and $263,874 in 2016. During the Relevant Period, Humann served as a member of the Compensation Committee.

32. Defendant Robert D. Marcus ("Marcus") has served as a director of the Company since November 1, 2013. Marcus received a sum of $471,083 in total compensation from Equifax from 2015 to 2016, including $229,108 in 2015, and $241,975 in 2016. During the Relevant Period, Marcus served as Chair of the Compensation Committee, and as a member of the Executive Committee and the Governance Committee.

33. Defendant Siri S. Marshall ("Marshall") has served as a director of the Company since August 7, 2006. Marshall received a sum of $495,631 in total compensation from Equifax from 2015 to 2016, including $242,878 in 2015, and $252,753 in 2016. During the Relevant Period, Marshall served as Chair of the Governance Committee, and as a member of the Executive Committee and the Compensation Committee.

34. Defendant John A. McKinley ("McKinley") has served as a director of the Company since October 1, 2008. McKinley received a sum of $500,767 in total compensation from Equifax from 2015 to 2016, including $245,358 in 2015, and $255,409 in 2016. During the Relevant Period, McKinley served as Chair of the Technology Committee, and as a member of the Audit Committee and the Executive Committee.

35. Defendant Elane B. Stock ("Stock") has served as a director of the Company since January 1, 2017. During the Relevant Period, Stock served as a member of the Technology Committee. Stock has been named as a member of the Demand Review Committee formed by the Board in response to Plaintiff's Demand.

36. Defendant Mark B. Templeton ("Templeton") has served as a director of the Company since February 8, 2008. Templeton received a sum of $481,358 in total compensation from Equifax from 2015 to 2016, including $236,308 in 2015, and $245,050 in 2016. During the Relevant Period, Templeton served as a member of the Audit Committee and the Technology Committee.

37. Defendants Smith, Gamble, Kelley, Ploder, Loughran, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton are, at times, collectively referred to herein as the "Individual Defendants."

38. Defendants Smith, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton are, at times, collectively referred to herein as the "Director Defendants."

39. Defendants Daleo, Hough, McKinley, and Templeton are, at times, collectively referred to herein as the "Audit Committee Defendants."

40. Defendants Feidler, Hough, McKinley, Stock, and Templeton are, at times, collectively referred to herein as the "Technology Committee Defendants."

41. Defendants Daleo, Humann, Marcus, and Marshall are, at times, collectively referred to herein as the "Compensation Committee Defendants."

42. Defendants Smith, Gamble, Kelley, Ploder, and Loughran are, at times, collectively referred to herein as the "Insider Selling Defendants."

IV. SUBSTANTIVE ALLEGATIONS

A. Description of Equifax's Business and Operations

43. One of the three major U.S. credit reporting agencies, Equifax is a global provider of information solutions and human resources business process outsourcing services for businesses, governments, and consumers. The Company's primary business involves compiling and maintaining databases of consumer financial data—i.e., credit, income, assets, debt, liquidity, net worth, spending activity, and employment—for use by businesses in assessing consumers'

creditworthiness. Accordingly, Equifax houses critically confidential and sensitive PII relating to the identity of all American citizens, including, *inter alia*, names, SSNs, birth dates, addresses, driver's license numbers, credit card numbers, and legal actions. Consumers have no choice in whether Equifax maintains their PII, and have no ability to protect their information Equifax possesses. While consumers have no choice as to whether, or how, Equifax maintains their PII, and have no ability to safeguard or protect their own information in Equifax's possession, Equifax is required by law to do so.

44. Equifax's primary business in the U.S. consists of tracking and rating the financial history of consumers. The Company maintains highly sensitive data such as loans, loan payments, credit card information, credit limits, credit terms, employment history, child support payments, and missed rent and utilities payments.

45. All of this highly sensitive information is then factored into credit reports that Equifax maintains and provides to financial companies, employers, and other entities that use those reports to assess the creditworthiness of, and make decisions about, individuals in a variety of areas.

46. Equifax's financial condition and prospects are dependent on protecting PII. The Company's Board and management are well aware of this vital obligation and have repeatedly represented to the public that the Company maintains "rigorous"

controls over risk management, data security, and cybersecurity, and that it is compliant with all applicable laws and regulations.

47. Today, Equifax organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data gathered from more than 7,100 employers.

48. Equifax also utilizes identity and authentication systems, known as "out of wallet" or "OOW" questions. These services can be utilized during initial account setup or password resets to "leverage" information "in most consumers' credit files to perform a reasonably strong authentication" by asking questions like "What was your address when you were 18?" and "Do you have an auto loan with a monthly payment of $245?"

49. These services involve consumers providing Equifax with PII as part of the consumers paying for, and Equifax providing, such services. In addition to providing services to individual consumers, Equifax also supplies identity verification services to the U.S. Social Security Administration ("SSA") and works with the federal Centers for Medicare and Medicaid Services to verify eligibility for health-insurance subsidies. These services include helping consumers check their Social Security benefits and request replacement Social Security cards, as well as to verify eligibility for subsidies to buy health insurance under the Affordable Care

Act. Equifax has previously stated that its "partnership will help protect the millions of online transactions the SSA manages annually."

B. The Data Breach

50. On September 7, 2017, after the close of trading and while news of Hurricane Irma was dominating media reports, the Individual Defendants caused the Company to issue a press release titled "Equifax Announces Cybersecurity Incident Involving Consumer Information," which was also filed as an exhibit to a current report on Form 8-K with the SEC (the "September 7, 2017 Press Release"), revealing that the Company had experienced a massive cyberattack from mid-May 2017 through July 2017, estimating that 143 million U.S. consumers were impacted, stating in pertinent part:

> For Immediate Release
> Sep 07, 2017
>
> **Equifax Announces Cybersecurity Incident Involving Consumer Information**
>
> **No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases**
>
> **Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers**
>
> ***Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers.*** Criminals exploited a U.S. website application vulnerability to gain access to certain files. ***Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The***

company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. ***While the company's investigation is substantially complete***, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and ***one that strikes at the heart of who we are and what we do***. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been

> potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. - 1:00 a.m. Eastern time.
>
> In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.
>
> Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.
>
> CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

51. On that same day, September 7, 2017, Bloomberg reported that Defendant Gamble and two other Equifax executives sold approximately $1.8 million dollars' worth of stock before the cyberattack was revealed, stating in part:

> Three Equifax Inc. senior executives sold shares worth almost $1.8 million in the days after the company discovered a security breach that may have compromised information on about 143 million U.S. consumers.
>
> The trio had not yet been informed of the incident, the company said late Thursday.
>
> The credit-reporting service said earlier in a statement that it discovered the intrusion on July 29. Regulatory filings show that on Aug. 1, Chief Financial Officer John Gamble sold shares worth $946,374 and Joseph Loughran, president of U.S. information solutions, exercised options to dispose of stock worth $584,099. Rodolfo Ploder, president of workforce solutions, sold $250,458 of stock on Aug. 2. None of the filings lists the transactions as being part of 10b5-1 scheduled trading plans.

52. According to public statements issued by the Individual Defendants, Equifax first learned of the Data Breach on July 29, 2017, when Equifax's security department observed suspicious network traffic associated with the consumer dispute website (where consumers could investigate and contest issues with their credit reports). The Company's CEO and Chairman of the Board of nearly 12 years, Defendant Smith later testified before the U.S. House Subcommittee on Digital Commerce and Consumer Protection, on October 3, 2017, that he was told about the Data Breach by the Company's Chief Information Officer ("CIO") on July 31, 2017, following "suspicious activity" being first noticed by "someone in security" on July 29 and July 30, 2017. Smith testified that he notified the "lead director" of the Board of the Data Breach on August 22, 2017, and that the full Board was briefed

on August 24, 2017. In prepared testimony, Smith provided the following chronology of events:

> On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used that software, which is called "Apache Struts," in its online disputes portal, a website where consumers can dispute items on their credit report.
>
> On March 9, Equifax disseminated the U.S. CERT notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.
>
> On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.
>
> Based on the investigation to date, it appears that the first date the attacker(s) accessed sensitive information may have been on May 13, 2017. The company was not aware of that access at the time. Between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache

Struts vulnerability. During that time, Equifax's security tools did not detect this illegal access.

On July 29, however, Equifax's security department observed suspicious network traffic associated with the consumer dispute website (where consumers could investigate and contest issues with their credit reports). In response, the security department investigated and immediately blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. The criminal hack was over, but the hard work to figure out the nature, scope, and impact of it was just beginning.

I was told about the suspicious activity the next day, on July 31, in a conversation with the Chief Information Officer. At that time, I was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues. I certainly did not know that personal identifying information ("PII") had been stolen, or have any indication of the scope of this attack.

On August 2, consistent with its security incident response procedures, the company: 1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; 2) reached out, though company counsel, to engage the independent cybersecurity forensic consulting firm, Mandiant, to investigate the suspicious activity; and 3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, working literally around the clock, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, how many consumers were affected, and what types of information was accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was

not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information; discover what data was exfiltrated from the company; and trace that data back to unique consumer information.

By August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

On August 15, I was informed that it appeared likely that consumer PII had been stolen. I requested a detailed briefing to determine how the company should proceed.

On August 17, I held a senior leadership team meeting to receive the detailed briefing on the investigation. At that point, the forensic investigation had determined that there were large volumes of consumer data that had been compromised. Learning this information was deeply concerning to me, although the team needed to continue their analysis to understand the scope and specific consumers potentially affected. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

A substantial complication was that the information stolen from Equifax had been stored in various data tables, so tracing the records back to individual consumers, given the volume of records involved, was extremely time consuming and difficult. To facilitate the forensic effort, I approved the use by the investigative team of additional computer resources that significantly reduced the time to analyze the data.

On August 22, I notified Equifax's lead member of the Board of Directors, Mark Feidler, of the data breach, as well as my direct reports who headed up our various business units. In special telephonic board meetings on August 24 and 25, the full Board of Directors was informed. We also began developing the remediation we would need to assist affected consumers, even as the investigation continued apace. From this point forward, I was updated on a daily – and sometimes

> hourly – basis on both the investigative progress and the notification and remediation development.
>
> On September 1, I convened a Board meeting where we discussed the scale of the breach and what we had learned so far, noting that the company was continuing to investigate. We also discussed our efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident. A mounting concern also was that when any notification is made, the experts informed us that we had to prepare our network for exponentially more attacks after the notification, because a notification would provoke "copycat" attempts and other criminal activity.
>
> By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information we believed had been stolen, and we continued our planning for a public announcement of a breach of that magnitude, which included a rollout of a comprehensive support package for consumers.

53. However, it was not until after the close of trading hours on September 7, 2017,—***nearly six weeks after the Data Breach was purportedly detected***—that the Individual Defendants caused the Company to disclose the Data Breach to the public for the very first time.

C. The Data Breach Was the Product of the Individual Defendants' Conscious Failures to Act in the Face of Known Duties to Act

54. The public soon learned that the Data Breach was no accident or fluke, but, rather, was the product of the Individual Defendants' conscious disregard of known, recent red flags concerning the Company's data security vulnerability.

55. As detailed further below, during the Relevant Period, the Individual Defendants knew or consciously disregarded that they were not discharging their

fiduciary obligations by knowingly and completely failing to undertake their responsibility to ensure Equifax was operating in compliance with federal, state, and municipal laws, rules, and regulations regulating data security.

56. Specifically, despite learning that its data security systems were insufficient and exposed, the Individual Defendants consciously failed to: (i) develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) develop, implement, and maintain proper data security systems, controls, and monitoring systems; (iv) develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) adequately assess the risks associated with the Company's data security; (vi) adequately assess the risks associated with the Company's executive compensation plan and revise the executive compensation plan to make sure executives were held accountable for legal costs associated with corporate trauma caused by their action or inaction; (vii) maintain adequate corporate accounting and corporate financial-reporting resources; (viii) adequately assess the risks associated with the Company's financial reporting; and (ix) maintain effective internal controls over financial reporting.

57. The Individual Defendants breached their duties by (i) failing to take the steps and opportunities to prevent and stop the Data Breach, (ii) failing to comply with industry standards for the safekeeping and maintenance of the personal and financial information, (iii) failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect personal and financial information, (iv) failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue, (v) failing to implement a compensation system which holds executives accountable for harm caused to the Company by their action and/or inaction, and (vi) failing to properly maintain their sensitive PII.

1. Defendants Regarded Data Security as Critical to Equifax's Success, and Repeatedly Emphasized that to Investors

58. Equifax and the other two major credit reporting agencies maintain more sensitive PII about consumers than almost any other U.S. corporation. In fact, according to media reports,[8] in recent years, Equifax has made a concerted effort to gain an advantage over other credit reporting companies, has moved to acquire more databases on Americans and then sell that data, including a trove of employment

[8] *E.g.*, Michael Rapoport and AnnaMaria Andriotis, *Equifax Lost Social Security Numbers But Still Works for the Social Security Administration*, The Wall Street Journal, https://www.wsj.com/articles/equifax-work-for-government-shows-companys-broad-reach-1505781393 (last visited Jan. 17, 2018).

records, in large part, due to its acquisition of Talx Corp. in 2007, and has expanded the number of people for which it had credit reports by paying $1 billion in 2012 to acquire Computer Science Corp.'s credit services unit, which gave it access to credit files for approximately 20% of the U.S. population.

59. Based on correspondence between the SEC and the Company's CEO and Board Chairman (Defendant Smith) and its former CFO (Lee Adrean), between at least 2011 and 2014, the SEC had scrutinized Equifax for inadequate disclosures of the Company's cyber-risk and poor overall disclosure controls. Specifically, in January 2014, the SEC probed Equifax's CEO and Board Chairman (Defendant Smith) about what the Company considered inadequate disclosures regarding a material weakness in Equifax's internal controls over financial reporting in 2013. In response, Equifax provided the SEC with a detailed timeline of its evaluation of the control weaknesses, from which it was concluded that its interim quarterly disclosure controls were also ineffective. Additionally, in September 2012, the SEC informed Equifax that in future filings, it needed to include more information about cyberattacks, security breaches, and other similar events it had experienced in the past, in order to "provide the proper context" for such disclosures. The Company agreed to add such additional details, including the statement that it had "not experienced any material breach of cybersecurity," but that if such incidents should

occur, it would potentially compromise Equifax's networks and that the information stored thereupon could be accessed, publicly disclosed, lost, and/or stolen.

60. During a Barclays Americans ("Barclays") Select Conference held May 18, 2016, Barclays Analyst, Manav Patnaik, specifically asked about Equifax's data security, inquiring: "[H]ow do you guys make sure the data doesn't bleed, and I guess you have a little bit of news with the W2 issues being- is that an issue? How should we think about that?" In response, Defendant Smith stressed the importance and purported strength of the Company's data security, explaining as follows:

> You know, ***data security is obviously for almost anyone, any business you're in, a top of mind. We have a world-class team, we never take for granted our need to continue to innovate around data security. I think we are in a very good position now***, but you can never become complacent as it relates to security, because a lot of people with a lot of time on their hands trying to crack that database. But all in all, we have come so far in ten years, as has the entire world, on data security.

61. During an Equifax International Business Unit Call hosted by Cowen and Company on November 30, 2016, the Head of Equifax's International Division, John Hartman, spoke on behalf of the Company, specifically regarding its data security, *inter alia*, explaining that "***we always want to be a trusted steward of the data and an advocate for with data, the people behind the data, and we work pretty hard to do that and keep all of our data secure. It's at the core of what we do***."

62. In its "risk factors" section of its latest annual report, filed on Form 10-K with the SEC on February 22, 2017, for the 2016 fiscal year (the "2016 10-K"), the Company warned "our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial of service or other advanced persistent attacks by hackers." The Company stated that "[u]nauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers."

63. The Company also stated that its "property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur" in the event that "such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations."

64. During the August 17 Terry College Speech, Smith frequently discussed security issues relating to the Company's large database. "When you have the size database we have, it's very attractive for others to try to get into our

database," admitted Smith, "[s]o it is a huge priority for us." Smith's fastest growing area of security concern was state-sponsored hacking and espionage. "It's countries you'd expect—you know it's China, it's Russia, it's Iran, Iraq—and they're being very aggressive trying to get access to the know-how about how companies have built their capabilities, and transport that know-how back to their countries," said Smith. "It's my number one worry," Smith confessed. During the speech, Smith was asked specifically about data fraud and security. "Fraud is a huge opportunity for us. It is a massive, growing business for us," he said.

65. Despite his knowledge of the Data Breach, Smith remained silent about it during the August 17, 2017 Terry College Speech. Commenting on the omission in an article[9] published September 25, 2017, following disclosure of the Data Breach, Edward Queen, from Emory University's Center for Ethics, said the answers seem to suggest a level of arrogance and disregard. "The disturbing thing was that he responded the way he did to the question of security breaches, about data breaches, when he knew that the company had already suffered a massive one," Queen said.

[9] Aaron Diamant, *Equifax CEO weeks before disclosing breach: 'The days are bright for Equifax'*, http://www.wsbtv.com/news/local/atlanta/equifax-ceo-weeks-before-disclosing-breach-the-days-are-bright-for-equifax/614695087 (last visited Jan. 10, 2018).

66. During testimony before Congress on October 3, 2017, Smith was asked by U.S. Congressman Tony Cardenas: "For everyone that's on your Equifax team, is there anything more important than protecting PII of the consumers?" Smith responded: "No, sir."' Smith also testified that Equifax "embarked upon a very aggressive ramp-up in creating a culture, creating processes investing in people, in tools ***to put security top of mind***."

2. Defendants Had Access to Information Regarding Frequently Occurring Cyber Attacks, Which Were Closely Tracked at the Company

67. Because of their advisory, executive, managerial, and directorial positions with Equifax, each of the Individual Defendants had access to material, adverse, and non-public information about the Company's unlawful business practices and operations, lack and/or failure of compliance policies and practices, artificially-inflated financials and stock price, faulty internal controls, and improper representations.

68. The Company's public filings prior to the Data Breach expressly confirm the directors' knowledge: (i) of the specific, grave, imminent, and ongoing risk of breach of the consumer data maintained by Equifax, (ii) of their duties and responsibilities to monitor and ensure that the Company's data security measures were developed, implemented, and maintained at all times in a manner sufficiently

adequate and reasonable to effectively protect and prevent against breach of its consumer data, and (iii) that a failure to undertake and fulfill their duties and responsibilities could have dire consequences to both Equifax and consumers.

69. For example, the Company's 2016 10-K—signed and authorized by ***all*** of Equifax's directors—provided, in pertinent part, as follows:

> ***Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.***[10]
>
> In the ordinary course of business, we rely upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including business-to-business and business-to-consumer electronic commerce and internal accounting and financial reporting systems. Additionally, ***we collect and store sensitive data, including*** intellectual property, proprietary business information and ***personally identifiable information of our customers,*** employees, consumers and suppliers, ***in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.***
>
> Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, ***our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to*** damage, disruptions, shutdowns, or ***breaches of confidential information due to criminal conduct, denial***

[10] Emphasis in original; all other emphases below are added by Plaintiff.

> ***of service or other advanced persistent attacks by hackers,*** employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. ***Unauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.***
>
> ***We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact.*** Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. ***Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations.*** Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Also, our third-party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

Precisely the same language also appeared in the Company's annual report, filed on Form 10-K with the SEC on February 24, 2016, for the 2015 fiscal year (the "2015 10-K"), also signed and authorized by ***all*** of Equifax's directors.

70. Having previously acknowledged that Equifax has been "regularly the target of attempted cyber and other security threats," the directors were thus aware—***prior to the Data Breach***—that the Company faced a specific, grave, imminent, and ongoing risk of breach of its consumer data. In light of this known risk, and the fact that data security is decidedly essential to Equifax's core business operations and strategy, the Individual Defendants also were aware—***prior to the Data Breach***—of their duties and responsibilities to monitor and ensure that the Company developed, implemented, and maintained sufficiently adequate, reasonable, and effective data security measures at all times to protect and prevent against further breach, as well as the potentially catastrophic harms that could result to Equifax and consumers from the Individual Defendants' failure to undertake and fulfill such duties and responsibilities.

3. The Individual Defendants Learned of Specific Cyber Attack Methods and Risks, Yet Consciously Disregarded Their Duties to Act

71. The Individual Defendants knew they were not discharging their fiduciary obligations to monitor and oversee the Company's data security systems, yet failed to act, demonstrating a conscious disregard for their duties.

72. Equifax experienced several prior hacking incidents and security vulnerabilities that placed the Board on notice that its data security systems and controls were grossly inadequate.

73. Time and time again, the Individual Defendants were presented with evidence that Equifax's cybersecurity measures were inadequate to protect consumers' sensitive financial and personal data from security breaches on at least two occasions, yet consciously failed to take appropriate action, including, but not limited to, failing to ensure even basic security patches were applied to the Company's security systems, and failing to ensure critical PII available through public-facing websites was encrypted.

74. An article published by *Network World* in 2007 detailed conversations with Equifax's then-Senior Vice President of Information Security, Anthony W. Spinelli, who the Company hired in 2005 to evaluate and enhance its admittedly-deficient data security. Spinelli explained some of the deficiencies he discovered in the Company's data security following his initial evaluation, noting that "[h]istorically, security [at Equifax] was very departmental," in that "[y]ou'll have one department that does compliance and has some security people, some [employees] doing access control, some other folks managing firewalls." Spinelli also conceded that, while Equifax "had a strong security program ***in pockets***, with

the new and emerging risks," it knew its data security was insufficient. Tellingly, even as far back as 2007, Gartner security analyst Rich Mogull prophesized that "[i]f someone attacks Equifax, they're going to come through the main door—their Web site."[11]

75. Spinelli worked closely with the Company's then-directors as part of his three-year plan to enhance the Company's data security. The *Network World* article noted in greater detail the Board's specific knowledge of, and direct involvement in, Spinelli's efforts to enhance Equifax's data security, providing, in pertinent part, as follows:

> Spinelli and his team created a "heat map" to clearly illustrate which areas of the company were less secure than others and prioritize fixes based on greatest need. Heat map in hand, ***Spinelli met with Equifax's board of directors just weeks after he was hired, to present the results of these assessments and pitch a three-year, $15 million plan to reorganize security.***
>
> * * *
>
> ***The board signed off on Spinelli's project, and 105 days after being hired, he began implementing his plan.*** The first step was tearing down the existing security organizations, determining staffers' core skills -- whether they were operations, data-loss prevention, engineering, compliance -- and regrouping them. Spinelli's $15 million project included adding 43 positions over the life of the three-year plan. He became the IT security leader of Equifax's new Security Council,

[11] *See* Cara Garretson, *Equifax Ratchets up Security*, Network World, https://www.networkworld.com/article/2298600/access-control/equifax-ratchets-up-security.html (last visited Jan. 8, 2017).

designed to ensure the goals of the IT security, data security and physical security departments are aligned.

* * *

With each technology expense, Spinelli wanted to be able to go back to the board and explain how the new hardware or software would heighten security. "For every initiative we wanted to do, say a firewall refresh, we had to explain how that improves one of those 10 [ISO 27001] tenets," he says.

* * *

Spinelli went back to the board of directors in November to report results for the first year of the plan. He revised his heat map to show where risks were mitigated. "We had gotten rid of all the high-risk areas," he says. "In '07 we'll do the medium ones, and in '08 the low-risk areas."

But although Spinelli's plan hit its targets for the first year, and he's optimistic about the remaining two, he knows that when it comes to discussing security with corporate executives, he needs to continuously manage expectations.

"I don't want to give them the sense that every security risk in the future is now covered," he says.

76. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated, "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability?...They are first-hand delivering information for the

fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau."[12]

77. In March 2013, Equifax confirmed "fraudulent and unauthorized access" to the financial files of four high-profile celebrities.[13] "We are aware of recent media reports pertaining to unauthorized access to files belonging to high-profile individuals. Equifax can confirm that fraudulent and unauthorized access to four consumer credit reports has occurred," a spokesman for Equifax wrote in a statement.

78. Equifax was breached when, between April 2013 and January 2014, a hacker was able to defeat the Company's identity verification process and gain unauthorized access to consumer credit reports maintained by Equifax.[14]

---

[12] Elinor Mills, *Equifax tax forms expose worker Social Security numbers*, CNET, https://www.cnet.com/news/equifax-tax-forms-expose-worker-social-security-numbers/ (last visited Jan. 10, 2018).

[13] Pierre Thomas, *Equifax Confirms Hackers Stole Financial Data, Launches Investigation*, ABC News, http://abcnews.go.com/Politics/equifax-confirms-hackers-stole-financial-data-launches-investigation/story?id=18715884 (last visited Jan. 10, 2018).

[14] *See A Brief History of Equifax Security Fails*, *infra* at n.34; *see also* Data Incident Notification Letter from Equifax to New Hampshire Attorney General Joseph Foster, Mar. 5, 2015, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf (last visited Jan. 8, 2018).

79. Also in 2014, Equifax left private encryption keys on its server, allowing anyone who accessed its server to access the encryption keys, thus allowing them to decrypt any encrypted data stored on Equifax's servers into its original, unencrypted form.[15]

80. In 2015, Equifax exposed the credit reports of at least hundreds of consumers to an unauthorized third party as a result of a so-called "technical error" that purportedly occurred during a software change.[16]

81. In 2016, Deloitte Touche Tohmatsu Limited ("Deloitte"), one of the "Big Four" accounting organizations and the largest professional services network in the world by revenue and number of professionals, conducted a security audit of Equifax's data security and found several problems, including a careless approach to patching systems, according to a former Equifax employee. "Nobody took that

[15] *See Equifax Breach: Timeline, International, Patching, Gender, PCI, Oh My!*, Risk Based Security, https://www.riskbasedsecurity.com/2017/09/equifax-breach-timeline-international-patching-gender-pci-oh-my/ (last visited Jan. 8, 2018); Brian Krebs, Twitter, https://twitter.com/briankrebs/status/908722014449520642 (last visited Jan. 8, 2018).

[16] *See Data Breach Reports - July 7, 2015*, Identity Theft Resource Center, http://www.lovemytool.com/files/databreachreports_7_7_2015.pdf (last visited Jan. 8, 2018); *see also* Data Incident Notification Letter from King & Spalding to New Hampshire Attorney General Joseph Foster, April 2, 2015, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf (last visited Jan. 8, 2018).

security audit seriously," a former cybersecurity team employee told Lorenzo Franceschi-Bicchierai, a reporter for Motherboard, a publication of Vice Media LLC. "Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking," according to the former employee.[17]

82. Between April 17, 2016 and March 29, 2017, Equifax reported to several affected customers that unauthorized access to customers' employee tax records occurred in connection with the Company's Workforce Solutions division known as The Work Number (formerly known as "TALX"). The attackers relied on Equifax's outdated and insufficient consumer authentication methods—attackers were able to reset the four-digit PIN given to customer employees as a password, and then steal W-2 tax data after successfully answering personal questions about those employees. The extent of the fraud perpetrated with the help of hacked TALX accounts is unclear, and Equifax refused requests to say how many consumers or payroll service customers may have been impacted by the authentication weaknesses. Based on letters sent pursuant to state data breach notification laws,

[17] *See* Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, Motherboard, https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning (last visited on Jan. 17, 2018).

the affected companies included at least defense contractor giant Northrop Grumman, staffing firm Allegis Group,[18] Northrop Grumman Corp.,[19] Saint-Gobain Corp.,[20] Erickson Living,[21] and the University of Louisville.[22]

83. These large-scale, extended, and numerous breaches resulted from inadequate data security measures that purported to protected customer-employees' W-2 data with only of a four-digit PIN, which could be, and in fact were, reset by

[18] *See Disclosure of Personally Identifiable Information Letter from Allegis Group to Maryland Attorney General Jeff Karberg*, Mar. 6, 2017, *available at*: http://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2017/itu-281065.pdf (last visited Jan. 8, 2018); Notice of Data Security Incident, *available at*: https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1267012616 (last visited Jan. 8, 2018).

[19] *See Notice of Data Breach Letter from Northrop Grumman*, Apr. 18, 2017, https://oag.ca.gov/system/files/Northrop%20Grumman%20Individual%20Notification%20Letter_64772036_1_0.PDF (last visited Jan. 9, 2018).

[20] *See Incident Notification Letter from Attorney Angelo A. Stio III on Behalf of Saint-Gobain Corp. to New Hampshire Attorney General Joseph Foster*, Apr. 13, 2017, *available at*: https://www.doj.nh.gov/consumer/security-breaches/documents/saint-gobain-20170413.pdf (last visited Jan. 9, 2018).

[21] *See Data Security Incident Letter from Attorney Nicholas A. Oldham on Behalf of TALX Corp. to New Hampshire Attorney General Joseph Foster*, May 15, 2017, *available at*: https://www.doj.nh.gov/consumer/security-breaches/documents/talx-20170515.pdf (last visited Jan. 9, 2018).

[22] *See* Shelby Brown, *Updated: Hackers Steal University Employee Tax Info*, The Louisville Cardinal, http://www.louisvillecardinal.com/2017/04/hackers-steal-university-employee-tax-info/ (last visited Jan. 9, 2018).

unauthorized third parties.[23] According to Gartner fraud analyst Avivah Litan, "[i]t's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN," as these breaches should and could have been easily prevented through common and simple measures, such as requiring two-factor authentication. International Computer Science Institute senior researcher Nicholas Weaver added that "this is exactly the sort of mass scale attack that even the most basic SMS-based 2-factor would block," and accordingly posited that "if the federal government is smart, they will consider suing Equifax for false returns filed using W2 information stolen from TALX customers."

84. On May 5, 2016, Equifax announced that TALX had experienced a breach of the PII—including names, addresses, SSNs, alternative identification numbers, wage and employment information, and other personal information—of 431,000 employees of another major Equifax business client, Kroger.[24] This

[23] *See* Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, Krebs on Security, https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/ (last visited Jan. 9, 2018).

[24] *See* Russell Grantham, *Equifax Sued Over Theft of Kroger Workers' Info*, The Atlanta Journal-Constitution, http://www.ajc.com/business/equifax-sued-over-theft-kroger-workers-info/cjwGCYI8bkCg1fFIRri93H/ (last visited Jan. 8, 2018); Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, Krebs on Security, https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last visited Jan. 8, 2018); *see also Data Breach Reports - 2016 End of Year Report*,

massive breach resulted from a "glaring security issue" with Equifax's W-2 Express website, specifically caused by the Company's decision to allow access to client-employees sensitive, confidential PII using PIN numbers consisting only of the last four digits of their SSNs and their four-digit birth years—which, according to *Forbes*, "[a] determined hacker could gather . . . [just] by scouring the web."[25] Kroger spokesman Keith Dailey stated, "As far as I know, it's the standard Equifax setup."[26]

85. Consequently, the affected employees filed class action lawsuits in Georgia federal court against Equifax and EWS-TALX,[27] and in Missouri federal court against EWS-TALX.[28] The actions asserted claims for, *inter alia*, negligence, negligence per se, and violation of the Georgia Security Breach Notification Act, O.C.G.A. § 10-1-912, *et seq.*, seeking monetary damages exceeding $5 million, and other relief. According to the complaints, "[t]he Data Breach occurred because

---

Identity Theft Resource Center, https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf (last visited Jan. 8, 2018).

[25] *See A Brief History of Equifax Security Fails*, *infra* at n.34.

[26] *See Crooks Grab W-2s from Credit Bureau Equifax*, *supra* at n.23.

[27] *See Yochanan v. Equifax, Inc., et al.*, No. 1:16-cv-01687-MHC (N.D. Ga.), filed May 24, 2016.

[28] *See Yochanan v. Equifax Workforce Solutions a/k/a TALX Corp.*, No. 4:16-cv-00843-CDP (E.D. Mo.), filed Jun 14, 2016 ("Missouri Action").

Equifax failed to implement adequate security measures to safeguard[] consumers' [PII] and willfully ignored ***known*** weaknesses in its data security, including prior hacks into its information systems."[29]

86. The complaints also alleged that "Equifax ha[d] yet to acknowledge the breach, or notify victims of the Data Breach," and "[a]ccording to a Kroger spokesman, other companies which rely upon Equifax for W-2 services may have also been subject to the Data Breach, as the inadequate security measures, . . . were the standard Equifax operating method." The complaints further alleged that the Company flouted its own promises and policies by failing to maintain adequate data security measures, which allowed that data breach to occur:

> With Regard to W-2s in particular, prior to the Data Breach, Equifax explained "[a]s W-2 data is sensitive and subject to federal regulations, every precaution is taken to ensure both security and accuracy. Equifax performs extensive testing and reviews before distribution." Equifax further reassured customers that "Equifax makes it easy to manage administration related to W-2s through web Manager. This user-friendly online tool is seamlessly integrated into all Equifax services, and ***can only be accessed by authorized staff members with a valid user ID and PIN***." Prior to the Data Breach, Equifax promised its customers and everyone about whom it collects PII that it would reasonably protect their PII. Equifax's privacy policy stated, in relevant part:

[29] Emphasis in original.

> "**EFFORTS WE MAKE TO SAFEGUARD YOUR PERSONAL INFORMATION**
>
> We are committed to protecting the security of your information through procedures and technology designed for this purpose by taking these steps:
>
> - We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you and to our customers. Employees who misuse information are subject to disciplinary action, including termination.
> - We have reasonable physical, technical and procedural safeguards to help protect your personal information.
> - In areas that contain your personal information, we use secure socket layer (SSL) encryption to help protect this information while it is in transit between our servers and your computer."

Equifax further cautioned small businesses utilizing its services to play the following role in protecting the security of their own information:

> **Choose your passwords carefully:** Always create a password that's easy for you to remember but difficult for someone else to figure out.

* * *

Despite that admonition, Defendant set default passwords and PIN numbers for its W-2 services as the last four digits of individual's social security numbers and the four digit year of birth for those individuals.

* * *

Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting businesses who have encountered a data breach.

> Equifax expressly advises businesses which have lost customer data to "Quickly Notify Those Affected"; "Provide Personalized Communication"; and "Offer Credit Protection." Despite those admonitions, to date, Equifax has not reached out to affected employees, and has not provided personalized communications to those affected, or offered credit protection to those whose W-2s were compromised by the Data Breach.

87. On September 30, 2016, the parties to the Missouri Action filed a Stipulation of Dismissal Without Prejudice, which stated, *inter alia*, "EWS has changed the authentication process that was the subject of this action. Employees of EWS customers are no longer allowed to use default PINs containing personally identifiable information to access their W-2 information."

88. In a statement released to data security blog Krebs On Security published May 6, 2016,[30] Equifax spokeswoman Dianne Bernez confirmed that the Company had been made aware of suspected fraudulent access to payroll information through its W-2 Express service by Kroger, but attempted to shift the blame:

> "The information in question was accessed by unauthorized individuals who were able to gain access by using users' personally identifiable information," the statement reads. "We have no reason to believe the personally identifiable information was attained through Equifax systems. Unfortunately, as individuals' personally identifiable information has become more publicly available, these types of online fraud incidents have escalated. As a result, it is critical for consumers and businesses to take steps to protect consumers' personally

[30] *Crooks Grab W-2s from Credit Bureau Equifax*, *supra* at n.23.

> identifiable information including the use of strong passwords and PIN codes. We are working closely with Kroger to assess and monitor the situation."

The Company's statement failed to explain why Equifax chose to use only the last four digits of employees' SSNs and birth year as the default verification information, why Equifax issued PII as the default pin codes without generating and issuing random codes that would able to be found elsewhere associated to the employee issued to, nor why Equifax otherwise failed to spend the resources necessary ensure basic data security, evidencing Defendants' complete disregard for the security of the employees' PII.

89. Also in 2016, another breach of Equifax's W-2 Express website resulted in the compromise of W-2 information for approximately 600 current and former employees of the University of Stanford.[31] Northwestern University also just alerted 150 employees that their salary and tax data was stolen via Equifax that year, using only a full SSN and birth date. In response, Equifax provided its credit monitoring services to Northwestern employees.[32]

---

[31] *See Data Breach Reports - 2016 End of Year Report*, *supra* at n.23; *see also* Hannah Knowles, *University Employees Vulnerable After Tax Data Breach*, The Stanford Daily, https://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/ (last visited Jan. 8, 2018).

[32] *Free Credit Monitoring, ID Theft Protection Offered To Employees*, Northwestern Now, https://news.northwestern.edu/stories/2016/05/free-credit-monitoring-id-theft-proection-offered-to-employees/ (last visited Jan. 10, 2018).

90. In December 2016, a security researcher, after scanning the Company's public-facing infrastructure for just a few hours, found a Company website that allowed the researcher to access ***the personal data of every American***, including SSNs, full names, birthdates, and city and state of residence. The site appeared as a portal made only for employees, but was in fact ***completely exposed*** to the public. The website displayed several search fields, and anyone—with no authentication whatsoever—could force the website to display the unencrypted personal data of every American.

91. The December 2016 security researcher incident is more particularly described in an October 26, 2017 article written by journalist Lorenzo Franceschi-Bicchierai that was based, in large part, on accounts of former Equifax employees that exposed the Company's knowledge of the vulnerabilities leading to the Data Breach:

> **Equifax Was Warned**
>
> **Last year, a security researcher alerted Equifax that anyone could have stolen the personal data of all Americans. The company failed to heed the warning.**
>
> Months before its catastrophic data breach, a security researcher warned Equifax that it was vulnerable to the kind of attack that later compromised the personal data of more than 145 million Americans, Motherboard has learned. Six months after the researcher first notified the company about the vulnerability, Equifax patched it—but only after

the massive breach that made headlines had already taken place, according to Equifax's own timeline.

This revelation opens the possibility that more than one group of hackers broke into the company. And, more importantly, it raises new questions about Equifax's own security practices, and whether the company took the right precautions and heeded warnings of serious vulnerabilities before its disastrous hack.

Late last year, a security researcher started looking into some of the servers and websites that Equifax had on the internet. In just a few hours, after scanning the company's public-facing infrastructure, the researcher couldn't believe what they had found. One particular website allowed them to access the personal data of every American, including social security numbers, full names, birthdates, and city and state of residence, the researcher told Motherboard.

The site looked like a portal made only for employees, but was completely exposed to anyone on the internet. It displayed several search fields, and anyone—with no authentication whatsoever—could force the site to display the personal data of Equifax's customers, according to the researcher. Motherboard saw multiple sets of the data they were able to access.

“I didn't have to do anything fancy,” the researcher told Motherboard, explaining that the site was vulnerable to a basic “forced browsing” bug. The researcher requested anonymity out of professional concerns.

“All you had to do was put in a search term and get millions of results, just instantly—in cleartext, through a web app,” they said. In total, the researcher downloaded the data of hundreds of thousands of Americans in order to show Equifax the vulnerabilities within its systems. They said they could have downloaded the data of all of Equifax's customers in 10 minutes: “I've seen a lot of bad things, but not this bad.”

While probing Equifax servers and sites, the researcher said that they were also able to take control—or get shell access as hackers refer to it—on several Equifax servers, and found several others vulnerable to simple bugs such as SQL injection, a common, basic way of attacking

sites. Many servers were running outdated software. According to one analysis performed in early September, Equifax had thousands of servers exposed on the internet, indicating both massive sprawl and loose control of its infrastructure, which increased the company's attack surface.

After discovering all these issues in December, the researcher said they immediately reported them to the company.

“It should’ve been fixed the moment it was found. It would have taken them five minutes, they could've just taken the site down,” they told me. “In this case it was just ‘please take this site down, make it not public.’ That's all they needed to do.”

According to the researcher, Equifax didn't take the site down until June.

Everyone knows what happened next.

On September 7, Equifax, the largest credit reporting agency in the United States, disclosed this massive hack of its internal systems. The firm, which, ironically, sells services to monitor data breaches, revealed hackers had stolen the sensitive personal data of 145.5 million Americans, including social security numbers, names, home addresses, and driver's license numbers. For many former Equifax employees, this breach came as no surprise.

Given that banks and other financial institutions rely on Equifax's data to verify the identity of potential customers seeking credit, this was a massive, damaging hack not only to the 145.5 million victims, but the whole US economy. Equifax has publicly blamed the breach on an unpatched vulnerability in the web application software Apache Struts and on one employee who failed to identify it and patch it on a specific consumer dispute portal.

The consumer dispute portal where Equifax says the breach happened is not the same one that the security researcher identified as vulnerable last year. But the type of data exposed is similar, and according to Equifax's own timeline, the vulnerable website discovered by the

researcher was still up when the company was hacked in May, and was still up three months after a reported separate breach.

The researcher's findings, in other words, showed there were multiple ways into Equifax's networks. Months later, the hackers, who stole the records of 145.5 million Americans and 700,000 Brits, exploited more than 30 different servers, according to Bloomberg. Considering all the bugs and vulnerabilities they identified, the anonymous security researcher is convinced Equifax wasn't just hacked by one group of attackers.

“If it took me three hours to find that website, I definitely think I'm not the only one who found it,” they said. “It wasn't just one breach. It was maybe dozens.”

Equifax declined to answer any specific questions about the researcher's findings. “As a matter of policy, Equifax does not comment publicly on internal security operations,” the company told me in a statement.

Data breaches are part of life, but given the sensitivity of the data Equifax handles, as well as the way it botched the breach's disclosure, many in the information security world say Equifax didn't do enough to keep our data safe.

That opinion is also held by many former Equifax employees, who told me the company didn't take security seriously enough.

Motherboard spoke to 14 former Equifax employees to gauge whether a spectacular hack like this one was something the company should’ve foreseen and prepared for. We granted anonymity to these employees because they signed nondisclosure agreements with the company. While there was no consensus, the majority of former employees, some of whom worked in the security team or alongside it, said a breach like this was inevitable.

“The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, to be preposterous,” said a former employee, who worked in IT at Equifax and is now a cybersecurity engineer.

"Being a trusted steward of data is vital to the mission of Equifax," the company's former CEO Richard Smith, who resigned in the wake of the data breach, told lawmakers during a hearing on October 4. "I've been there for 12 years, Mr. Chairman, and we embarked upon a very aggressive ramp-up in creating a culture, creating processes investing in people, in tools to put security top of mind."

Another former employee, who was part of the cybersecurity team and left the company this year, said that Equifax hired Deloitte last year to do a security audit. The audit found several problems, including a careless approach to patching systems, according to the former employee.

"Nobody took that security audit seriously," the former cybersecurity team employee told me. "Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking."

When I asked a current employee on the cybersecurity team to confirm this fact, they replied that they weren't sure about Deloitte specifically because Equifax brings in security consultants regularly. A Deloitte spokesperson declined to comment, saying "confidentiality prohibits us from confirming or discussing client engagements."

Equifax declined to answer a series of specific question for this story. Instead, a spokesperson sent the following statement:

"As a matter of policy, Equifax does not comment publicly on internal security operations. However, as our former CEO recently testified to Congress, Equifax has in the past conducted thorough security reviews using expert external review teams," the statement read. "He further testified that Equifax expended significant resources to install industry standard cybersecurity defenses and put in place processes to address vulnerabilities. Since the recent breach, additional remediation steps have been taken. It is incorrect to suggest reports were ignored."

Perhaps, Equifax's disastrous data breach was a foregone conclusion, given the company's history of security mishaps. Some of the former employees we spoke to had specific stories about vulnerabilities that

remained unpatched, internal portals that weren't as secure as they should have been, and infrastructure that didn't require two-factor authentication to log in to.

One year, according to the former employee who worked in IT, he and his team found that someone had programmed files to be inappropriately wiped on multiple servers—an act of internal sabotage, he said. But the team had no way of discovering who did it—there were no activity logs or ways to track who had set up the script.

“Luck is what found it,” he said. “It isn't like [Equifax] had file integrity monitoring or anything like that to discover it—not even on systems with sensitive information.”

These issues have been the norm at Equifax, according to the people I spoke to. One person, who worked at Equifax around 10 years ago, recalled that during his time there he warned the company of some servers that needed to be patched because they had open file-sharing ports that could be exploited by worms. The company did nothing, and, three months later, some servers got infected with the infamous Conficker worm, the source said.

“It's the same problem, but 10 years later,” the source said.

As Bloomberg reported in September, Equifax employees were so worried a hack might be coming that they used to joke that the over-100-year-old company was just one hack away from bankruptcy.

“It's a strange company. Given the amount of data they have access to and the sensitivity of it, security isn't at the forefront of everybody’s mind, not how it should be,” another former Equifax cybersecurity employee told me. “It was always a bit of a struggle there to get anything done.”

The anonymous researcher who could've downloaded all Americans’ data knows this very well.

“I couldn't believe it, it was shocking,” they told me. “It was just disgusting to see them take this long to do anything about it.”

92. Thus, while probing Equifax servers and sites in December 2016, the security researcher was also able to take control—or get "shell access"—to several Equifax servers. The researcher also found several other Equifax websites vulnerable to common and basic attacks such as SQL injections. In addition, many servers were running outdated software. In fact, Equifax had thousands of servers exposed on the internet, indicating both massive sprawl and deficient control of its infrastructure, which increased the Company's vulnerability to attacks.

93. Upon discovering these issues in December 2016, the security researcher immediately reported the issues to Equifax. Rather than acting swiftly on that warning, Equifax instead waited six months to fix the security flaw identified by the researcher—critically deficient protections on a public-facing web application—but by then, it was too late and allowed downloading the data of every Equifax customer in 10 minutes. The security researcher accordingly warned Equifax that one of its public-facing websites "displayed several search fields, and anyone—with no authentication whatsoever—could force the site to display the personal data of Equifax's customers . . . ." But Equifax did not patch the vulnerability for approximately ***six months***, despite the fact "[i]t should have been

fixed the moment it was found" and "would have taken [the Company] five minutes," or Equifax simply "could have just taken the site down."[33]

94. By the time the vulnerability was addressed, the Data Breach—accomplished by the same type of attack warned of by the security researcher in December 2016—had already occurred.

95. Given how the Data Breach was brought to Smith's attention—according to the Company, within two days of Equifax's security team noticing "suspicious network traffic," and well before the scope of the Data Breach was known—it is reasonable to infer that the December 2016 security researcher's intrusion were just as swiftly brought to the attention of the Individual Defendants. Yet, the Individual Defendants did nothing in response until the harm from the Data Breach had already occurred.

96. Indeed, Equifax's security was rated poorly since at least the beginning of 2017, receiving a FICO enterprise security score around 550 on a scale ranging from 300 to 850. That score comprises assessments of security relating to hardware, network security, and web services. Despite Equifax's purported data security expertise, four cyber-risk analysis companies reported in The Wall Street Journal that Equifax "was behind on basic maintenance of websites that could have been

[33] *See Equifax Was Warned*, *supra* at n.16.

involved in transmitting sensitive consumer information and scored poorly in areas" highly relevant to potential breaches.[34]

97. In February 2017, Equifax disclosed another "technical issue" that compromised credit information belonging to some consumers who used identity theft protection services from its customer, LifeLock.

98. In February 2017, the same month that the directors caused the Company to file its 2016 10-K, Equifax disclosed that a so-called "technical issue" resulted in the disclosure, to an unauthorized third party, of the credit information of at least 158 consumers who used identity theft protection services from one of Equifax's major business clients, LifeLock.[35]

[34] AnnaMaria Andriotis and Robert McMillan, *Equifax Security Showed Signs of Trouble Months Before Hack*, The Wall Street Journal, https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947 (last visited Jan. 11, 2018).

[35] *See Equif*@#$d: Equifax Breach Response Off To A Rough Start*, Risk Based Security, https://www.riskbasedsecurity.com/2017/09/equifd-equifax-breach-response-off-to-a-rough-start/ (last visited Jan. 8, 2018); Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, Forbes, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#5a3ffae7677c (last visited Jan. 8, 2018); *see also* Data Incident Notification Letter from King & Spalding to New Hampshire Attorney General Joseph Foster, *supra* at n.15.

99. On March 8, 2017, U.S.-CERT sent Equifax a notice of the need to patch a particular vulnerability in the Apache Struts 2 software used by Equifax.

100. In March or April 2017, Mandiant alerted Equifax to the fact that its unpatched systems and misconfigured security policies could indicate major problems. This warning was described in a September 29, 2017 Bloomberg article[36] based on "interviews with more than a dozen people familiar with twin probes being conducted by Equifax and U.S. law enforcement." The article reports, *inter alia*:

> In the corridors and break rooms of Equifax Inc.'s giant Atlanta headquarters, employees used to joke that their enormously successful credit reporting company was just one hack away from bankruptcy. They weren't being disparaging, just darkly honest: Founded in the 19th century as a retail credit company, Equifax had over the years morphed into one of the largest repositories of Americans' most sensitive financial data, which the company sliced and diced and sold to banks and hedge funds. In short, the viability of Equifax and the security of its data were one and the same.
>
> Nike Zheng, a Chinese cybersecurity researcher from a bustling industrial center near Shanghai, probably knew little about Equifax or the value of the data pulsing through its servers when he exposed a flaw in popular backend software for web applications called Apache Struts. Information he provided to Apache, which published it along with a fix on March 6, showed how the flaw could be used to steal data from any company using the software.

[36] Michael Riley, Jordan Robertson, and Anita Sharpe, *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, Bloomberg Businessweek, https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros (last visited on Jan, 17, 2018).

The average American had no reason to notice Apache's post but it caught the attention of the global hacking community. Within 24 hours, the information was posted to FreeBuf.com, a Chinese security website, and showed up the same day in Metasploit, a popular free hacking tool. On March 10, hackers scanning the internet for computer systems vulnerable to the attack got a hit on an Equifax server in Atlanta, according to people familiar with the investigation.

Before long, hackers had penetrated Equifax. They may not have immediately grasped the value of their discovery, but, as the attack escalated over the following months, that first group—known as an entry crew—handed off to a more sophisticated team of hackers. They homed in on a bounty of staggering scale: the financial data—Social Security numbers, birth dates, addresses and more—of at least 143 million Americans. By the time they were done, the attackers had accessed dozens of sensitive databases and created more than 30 separate entry points into Equifax's computer systems. The hackers were finally discovered on July 29, but were so deeply embedded that the company was forced to take a consumer complaint portal offline for 11 days while the security team found and closed the backdoors the intruders had set up.

The handoff to more sophisticated hackers is among the evidence that led some investigators inside Equifax to suspect a nation-state was behind the hack. Many of the tools used were Chinese, and these people say the Equifax breach has the hallmarks of similar intrusions in recent years at giant health insurer Anthem Inc. and the U.S. Office of Personnel Management; both were ultimately attributed to hackers working for Chinese intelligence.

Others involved in the investigation aren't so sure, saying the evidence is inconclusive at best or points in other directions. One person briefed on the probe being conducted by the Federal Bureau of Investigation and U.S. intelligence agencies said that there is evidence that a nation-state may have played a role, but that it doesn't point to China. The person declined to name the country involved because the details are classified. Mandiant, the security consulting firm hired by Equifax to investigate the breach, said in a report distributed to Equifax clients on

Sept. 19 that it didn't have enough data to identify either the attackers or their country of origin.

Wherever the digital trail ultimately leads, one thing is clear: The scant details about the breach so far released by Equifax—besides angering millions of Americans—omit some of the most important elements of the intrusion and what the company has since learned about the hackers' tactics and motives. Bloomberg has reconstructed the chain of events through interviews with more than a dozen people familiar with twin probes being conducted by Equifax and U.S. law enforcement.

In one of the most telling revelations, Equifax and Mandiant got into a dispute just as the hackers were gaining a foothold in the company's network. That rift, which appears to have squelched a broader look at weaknesses in the company's security posture, looks to have given the intruders room to operate freely within the company's network for months. According to an internal analysis of the attack, the hackers had time to customize their tools to more efficiently exploit Equifax's software, and to query and analyze dozens of databases to decide which held the most valuable data. The trove they collected was so large it had to be broken up into smaller pieces to try to avoid tripping alarms as data slipped from the company's grasp through the summer. In an e-mailed statement, an Equifax spokesperson said: "We have had a professional, highly valuable relationship with Mandiant. We have no comment on the Mandiant investigation at this time."

The massive breach occurred even though Equifax had invested millions in sophisticated security measures, ran a dedicated operations center and deployed a suite of expensive anti-intrusion software. The effectiveness of that armory appears to have been compromised by poor implementation and the departure of key personnel in recent years. But the company's challenges may go still deeper. One U.S. government official said leads being pursued by investigators include the possibility that the hackers had help from someone inside the company. "We have no evidence of malicious inside activity," the Equifax spokesperson said. "We understand that law enforcement has an ongoing investigation."

The nature of the attack makes it harder to pin on particular perpetrators than either the Anthem or OPM hacks, said four people briefed on the probe. The attackers avoided using tools that investigators can use to fingerprint known groups. One of the tools used by the hackers—China Chopper—has a Chinese-language interface, but is also in use outside China, people familiar with the malware said.

The impact of the Equifax breach will echo for years. Millions of consumers will live with the worry that the hackers—either criminals or spies—hold the keys to their financial identity, and could use them to do serious harm. The ramifications for Equifax and the larger credit reporting industry could be equally severe. The crisis has already claimed the scalp of Richard Smith, the chief executive officer. Meanwhile, the federal government has launched several probes, and the company has been hit with a flurry of lawsuits. "I think Equifax is going to pay or settle for an amount that has a 'b' in it," says Erik Gordon, a University of Michigan business professor.

When Smith became Equifax CEO in 2005, the former General Electric Co. executive was underwhelmed by what he found. In a speech at the University of Georgia last month, he described a stagnating credit reporting agency with a "culture of tenure" and "average talent." However, Smith also saw enormous potential because Equifax inhabited a uniquely lucrative niche in the modern global economy.

In the speech, Smith explained that the company gets its data for free (because regular consumers hand it over to the banks when they apply for credit). Then, he said, the company crunches the data with the help of computer scientists and artificial intelligence and sells it back to the banks that gave Equifax the data in the first place. The business generates a gross margin of about 90 percent. "That's a pretty unique model," Smith said.

And one that he fully exploited. Smith acquired two dozen companies that have given Equifax new ways to package and sell data, while expanding operations to 25 countries and 10,000 employees. Business was good—the company's stock price quadrupled under Smith's watch, before the breach was announced—and its leaders lived well.

Equifax executives were prone to bragging about their mansions and expensive gadgets. They took lavish trips to Miami, where they stayed in luxury hotels costing as much as $1,000 a night. Last year, Smith's compensation was almost $15 million.

But the man who transformed Equifax was plagued each and every day by the fear that hackers would penetrate the company's firewall and make off with the personal data of millions of people. By the time he gave the speech on Aug. 17, Smith knew of the hack but the public didn't. He told the audience the risk of a breach was "my No. 1 worry" and lingered on the threats posed by spies and state-sponsored hackers.

Not long after becoming CEO, he hired Tony Spinelli, a well-regarded cyber expert, to overhaul the company's security. The new team rehearsed breach scenarios, which involved 24-hour crisis-management squads taking turns to address each given issue until it was resolved. Protocol included alerting the chief of security, who determined the severity of the breach, and then telling the executive leadership if a threat was considered serious.

Apparently, gaps remained. After the breach became public in September, Steve VanWieren, a vice president of data quality who left Equifax in January 2012 after almost 15 years, wrote in a post on LinkedIn that "it bothered me how much access just about any employee had to the personally identifiable attributes. I would see printed credit files sitting near shredders, and I would hear people speaking about specific cases, speaking aloud consumer's personally identifiable information."

Spinelli left in 2013, followed less than a year later by his top deputy, Nick Nedostup. Many rank and file followed them out the door, and key positions were filled by people who were not well-known in the clubby cybersecurity industry. The company hired Susan Mauldin, a former security chief at First Data Corp., to run the global security team. Mauldin introduced herself to colleagues as a card-carrying member of the National Rifle Association, according to a person familiar with the changes.

Two people who worked with Mauldin at Equifax say she seemed to be putting the right programs in place, or trying to. "***Internally***, ***security was viewed as a bottleneck***," one person said. "There was a lot of pressure to get things done. Anything related to IT was supposed to go through security." Mauldin couldn't be reached for comment.

The company continued to invest heavily in state-of-the-art technology, and had a dedicated team to quickly patch vulnerabilities like the one identified by Zheng. Overseeing technology for Equifax was David Webb, a Kellogg MBA and Russian-language major hired in 2010 from Silicon Valley Bank, where he had been chief operations officer. But one former security leader said he finally joined the talent exodus because it felt like he was working with the "B team."

Lapses in security began to catch up to the company in myriad ways beginning early this year. Since at least Feb. 1, Equifax had been aware that identity thieves were abusing a service that manages payroll data for companies, according to notices sent to victims.

Criminals were feeding stolen Social Security numbers and other personal information into login pages for Equifax Workforce Solutions, downloading W-2 and other tax forms for dozens of employees of clients including Northrop Grumman Corp., Whole Foods Market Inc. and Allegis Global Solutions Inc., a human resources company. They accessed the data freely for over a year to file fraudulent tax returns and steal the refunds before Equifax learned of the incidents. (KrebsOnSecurity.com, a cybersecurity blog, first reported the thefts in May.)

Equifax hired Mandiant in March to investigate any security weaknesses related to the scams, and in notifications mailed to victims throughout the summer, Equifax eventually said its systems weren't breached to acquire the personal data used in the fraud.

However, there are signs that Smith and others were aware something far more serious was going on. The investigation in March was described internally as "a top-secret project" and one that Smith was overseeing personally, according to one person with direct knowledge of the matter.

The relationship with Mandiant broke down sometime over the next several weeks—a period that would later turn out to be critical in how the breach unfolded. Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said. For its part, Equifax believed Mandiant had sent an undertrained team without the expertise it expected from a marquee security company. A Mandiant spokesman declined to comment on the March investigation.

Although the hackers inside Equifax were able to evade detection for months, once the hack was discovered on July 29, investigators quickly reconstructed their movements down to the individual commands they used. The company's suite of tools included Moloch, which works much like a black box after an airliner crash by keeping a record of a network's internal communications and data traffic. Using Moloch, investigators reconstructed every step.

Once the hackers found the vulnerability Zheng reported, they installed a simple backdoor known as a web shell. It didn't matter if Equifax fixed the vulnerability after that. The hackers had an invisible portal into the company's network. The Moloch data suggests the initial group of hackers struggled to jump through internal roadblocks like firewalls and security policies, but that changed once the advanced team took over. Those intruders used special tunneling tools to slide around firewalls, analyzing and cracking one database after the next—while stockpiling data on the company's own storage systems.

Besides amassing data on nearly every American adult, the hackers also sought information on specific people. It's not clear exactly why, but there are at least two possibilities: They were looking for high-net-worth individuals to defraud, or they wanted the financial details of people with potential intelligence value.

Eventually the intruders installed more than 30 web shells, each on a different web address, so they could continue operating in case some were discovered. Groups known to exploit web shells most effectively include teams with links to Chinese intelligence, including one nicknamed Shell Crew. Some investigators within Equifax reached the

conclusion that they were facing Chinese state hackers relatively quickly after analyzing the Moloch data, according to a person briefed on those discussions. If the Equifax breach was a purely criminal act, one would expect at least some of the stolen data, especially the credit card numbers that were taken, to have showed up for sale on the black market. That hasn't happened.

What's more, banks are typically asked to shut down all stolen cards if investigators are near certain who is behind a hack. In this case, they still aren't sure. That's why on Sept. 11, the FBI asked several major banks to monitor the credit card accounts of small batches of consumers—in one case just 20 people—for suspicious activity. Investigators were still looking for anything that could give them insight into the hackers' identity and motives, according to security experts.

"This wasn't a credit card play," said one person familiar with the investigation. "This was a 'get as much data as you can on every American' play." But it probably won't be known if state hackers—from China or another country—were involved until U.S. intelligence agencies and law enforcement complete their work.

That could take weeks or months, but Equifax is already a changed company. Smith has handed the reins to Paulino do Rego Barros, who will be interim CEO until the board finds a permanent replacement. Smith's departure was preceded by the early retirement of the company's two top security officials, chief information officer Webb and chief security officer Mauldin.

Federal investigators are probing suspicious stock sales by other executives that happened not long after Equifax discovered the breach, and the company's board has formed a special committee to review those share sales. "Equifax takes these matters seriously," the company said in its response to questions posed by Democrats on the House Energy and Commerce Committee. Meanwhile, lawmakers are making ominous noises about boosting oversight of the credit reporting industry, which is largely unregulated.

> "What member of Congress can vote against tighter regulation when every congressional district has nearly half its voters affected by this?" says Gordon, the Michigan business professor. "The lobbying wins when there is no organized group fighting back, but you don't need an organized group when you have 143 million angry people."

101. In April 2017, cyber-risk analysis firm Cyence assessed the risk of a data breach at Equifax in the next 12 months at 50%, ranking it second-to-last in its peer group of 23 companies.

102. In mid-July 2017, Equifax's FICO enterprise security score hit a low of approximately 475.

103. Security researchers have also discovered that the Company has been utilizing outdated technologies that are vulnerable to breach and exploitation. As noted in a *Forbes* article published following the Data Breach,

> [t]he good-guy hackers have found myriad old technologies running the Equifax site, many of which could be vulnerable to cyberattack. Researcher Kenneth White discovered a link in the source code on the Equifax consumer sign-in page that pointed to Netscape, a web browser that was discontinued in 2008. Kevin Beaumont, a British security pro who's spent 17 years helping protect businesses, found decade-old software in use . . . .

Another security researcher explained that Equifax was running "[o]ld IT systems[, which] could indicate lack of 'renewal' procedures, old and unpatched software," and "[i]t really looks like they don't care about security on their website - not surprised they got breached, certainly easily." And a cybersecurity engineer

discovered that Equifax was using out-of-date Java software, and concluded that "[i]t definitely should not be possible to do what happened if security was sound."[37]

104. Still, despite these known issues, the Individual Defendants utterly failed to, *inter alia*, (i) encrypt critically sensitive PII available through public-facing portals, or (ii) ensure critical patches were timely applied.

105. These numerous incidents discussed in § IV.C *supra*, in and of themselves, should have independently alerted the Board and management to the lack of data security at the Company, but, certainly in combination with one another, should have made the Company's directors further aware of the fact that (if they were undertaking and fulfilling, rather than utterly disregarding, their duties and responsibilities to monitor and ensure the adequacy, reasonableness, and efficacy of the Company's data security) there were specific, grave, imminent, and ongoing risks, not only of further breaches of the Company's consumer data, but as potential for a catastrophic breach of such information, and should have prompted immediate action by the Board and management to monitor and ensure that the Company developed, implemented, and maintained sufficiently adequate, reasonable, and effective data security measures to protect and prevent against further breaches, including the catastrophic Data Breach that ultimately occurred.

[37] *See A Brief History of Equifax Security Fails*, *supra* at n.34

106. The Individual Defendants' pre-Data Breach knowledge of the above-described risk of further consumer data breach, their duties and responsibilities to monitor and ensure that the Company protected and prevented against the same, and the consequences of their failure to do so, is further demonstrated by the fact that the Individual Defendants were involved in developing, and/or monitoring the development of, at least ***some*** data security measures from approximately 2005 to 2008, but, then in the nearly 10 years thereafter, utterly failed to subsequently undertake and fulfill their continuing duties and responsibilities to monitor and ensure that the Company's data security measures remained, and were maintained at all times, in a sufficiently adequate, reasonable, and effective manner to protect and prevent against further breaches.

4. Post-Data Breach Revelations and Admissions Confirm Defendants' Misconduct

107. On September 12, 2017, Smith published an op-ed in USA Today,[38] in which he made the following admissions:

> Equifax CEO: 'We will make changes'
>
> Last Thursday evening we announced a cybersecurity breach potentially impacting 143 million U.S. consumers. It was a painful announcement because of the concern and frustration this incident has

[38] Richard F. Smith, Equifax *CEO: 'We will make changes'*, USA Today, https://www.usatoday.com/story/opinion/2017/09/12/equifax-ceo-we-make-changes-editorials-debates/659738001/ (last visited Jan. 17, 2018).

created for so many consumers. We apologize to everyone affected. This is the most humbling moment in our 118-year history.

Equifax Security first discovered the intrusion on July 29. Understandably, many people are questioning why it took six weeks to report the incident to the public. Shortly after discovering the intrusion, we engaged a leading cybersecurity firm to conduct an investigation.

At the time, we thought the intrusion was limited. The team, working with Equifax Security personnel, devoted thousands of hours during the following weeks to investigate.

Our top priority is doing everything we can to support affected consumers. Our team is focused on this effort, and we are engaged around the clock in responding to millions of inquiries from consumers. Importantly, outside investigators found no evidence of unauthorized activity on our core consumer or commercial credit reporting databases.

We strongly recommend that every consumer visit our website (www.equifaxsecurity2017.com) to determine if their data is at risk. As of Tuesday, more than 15 million people have visited the website and 11.5 million are enrolling in credit file monitoring and identity theft protection.

We took the unprecedented step of offering credit file monitoring and identity theft protection to every U.S. consumer. Every consumer, whether affected or not, has the option of signing up for the services.

Consumers and media have raised legitimate concerns about the services we offered and the operations of our call center and website. We accept the criticism and are working to address a range of issues.

We are devoting extraordinary resources to make sure this kind of incident doesn't happen again. We will make changes and continue to strengthen our defenses against cyber crimes. We will make sure every consumer who wants protection has a full package of services. And we will continue to update everyone on our progress.

108. Several key Equifax executives were allowed to "retire" within weeks of the Data Breach revelation, including: (i) Smith, effective September 26, 2017; (ii) the Company's Chief Security Officer ("CSO") of over four years, Susan Mauldin, on September 15, 2017; and (iii) the Company's CIO of over seven years, David C. Webb, on September 15, 2017.

109. On September 15, 2017, a bipartisan group of attorneys general, including Georgia's attorney general, sent a letter[39] to Equifax outlining an array of concerns and requested actions. The letter noted concerns with Equifax's offer of free credit monitoring:

> Initially, in order to enroll in the free credit monitoring that Equifax offered to all Americans, it appeared that Equifax attached certain conditions to the offer, including mandatory arbitration, among other things. The fact that Equifax's own conduct created the need for these services demands that they be offered to consumers without tying the offer to complicated terms of service that may require them to forgo certain rights. It was not until after urging from our offices and public condemnation that Equifax withdrew these objectionable terms from its offer of free credit monitoring.
>
> * * *
>
> We believe continuing to offer consumers a fee-based service in addition to Equifax's free monitoring services will serve to only confuse consumers who are already struggling to make decisions on how to best protect themselves in the wake of this massive breach.

[39] https://law.georgia.gov/sites/law.georgia.gov/files/related_files/press_release/Equifax.Letter%20to%20Counsel.9-15-17.pdf (last visited Jan. 12, 2018).

110. On September 17, 2017, it was reported by Brian Krebs in an article entitled, "Ayuda! (Help!) Equifax Has My Data!"[40], that an online portal designed to let Equifax employees in Argentina manage credit report disputes from consumers in Argentina was "wide open, protected by perhaps the most easy-to-guess password combination ever: 'admin/admin.'" Equifax reportedly took the portal down immediately after being contacted by Krebs.

111. On September 26, 2017, the Company announced Smith would be allowed to "retire" as Chairman and CEO of the Company. The Company and Smith entered into an agreement, dated September 25, 2017 (the "Agreement"), in connection with his retirement, which modified his existing employment agreement. The Company and Smith agreed to disclaim any right to receive an annual bonus for the period ending December 31, 2017, and that "all decisions relating to the characterization of Mr. Smith's departure and any obligations or benefits owed to Mr. Smith under the Employment Agreement or any plan, program, policy, or practice of the Company will be deferred until the Board of Directors completes that review."

[40] *See* Brian Krebs, *Ayuda! (Help!) Equifax Has My Data!*, Krebs on Security, https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/ (last visited Jan. 17, 2018).

112. If Smith had been removed from his position, he would have received severance in the amount of $5 million. Because the Board retains the right to change the basis of his departure to a "for cause" termination, Smith may yet receive that compensation. Because Smith's "award agreements are still outstanding," according to a Company spokesperson, Smith might also retain the rights to millions of dollars in stock that have yet to vest, and the total amount of that award is "less than $20 million," according to the spokesperson.[41] Of course, in the months leading up to the Data Breach, and while the conditions at the Company were ripe for such a breach, Smith was able to unload $64,639,216.70 worth of his personally-held Equifax stock (approximately 73% of his total holdings) at artificially-inflated prices.

113. On September 27, 2017, newly-appointed Company interim CEO Paulino do Rego Barros, Jr. published an op-ed in the Wall Street Journal entitled, "On Behalf of Equifax, I'm Sorry."[42] In the article, Barros admitted, *inter alia*, that:

[41] *See* Maria Lamagna, *After breach, Equifax CEO leaves with $18 million pension, and possibly more*, Market Watch, https://www.marketwatch.com/story/equifax-ceo-leaves-with-18-million-pension-and-maybe-more-2017-09-26 (last visited Jan. 10, 2018).

[42] https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253 (last visited Jan. 10, 2018).

"We didn't live up to expectations." In the article, Barros made the following admissions:

> **On Behalf of Equifax, I'm Sorry**
>
> A new free service will let consumers lock or unlock access to their credit data any time they like.
>
> On behalf of Equifax, I want to express my sincere and total apology to every consumer affected by our recent data breach. People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations.
>
> We were hacked. That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key consumer questions were too often delayed, incomplete or both. We know it's our job to earn back your trust.
>
> We will act quickly and forcefully to correct our mistakes, while simultaneously developing a new approach to protecting consumer data. In the near term, our responsibility is to provide timely, reassuring support to every affected consumer. Our longer-term plan is to give consumers the power to protect and control access to their personal credit data.
>
> I was appointed Equifax's interim chief executive officer on Tuesday. I won't pretend to have figured out all the answers in two days. But I have been listening carefully to consumers and critics. I have heard the frustration and fear. I know we have to do a better job of helping you.
>
> Although we have made mistakes, we have successfully managed a tremendous volume of calls and clicks. And we're getting better each day. But it's not enough. I've told our team we have to do whatever it takes to upgrade the website and improve the call centers.

We have started work on our website, and I see significant signs of progress. I won't accept anything less than a superior process for consumers. We will make this site right or we will build another one from scratch. You have my word.

The same goes for the call centers. There is no excuse for delayed calls or agents who can't answer key questions. We will add agents and expand training until calls are answered promptly and knowledgeably. I will personally review a daily report on their operations.

We will also extend the services we are offering consumers. We have heard your concern that the window to sign up for free credit freezes with Equifax is too brief, so we are extending the deadline to the end of January. Likewise, we are extending the sign-up period for TrustedID Premier, the complimentary package we are offering all U.S. consumers, through the end of January.

We hope these immediate actions will go a long way toward addressing the concerns we are hearing from consumers. We know they won't solve the larger problem. We have to see this breach as a turning point—not just for Equifax, but for everyone interested in protecting personal data. Consumers need the power to control access to personal data.

Critics will say we are late to the party. But we have been studying and developing a potential solution for some time, as have others. Now it is time to act.

So here is our commitment: By Jan. 31, Equifax will offer a new service allowing all consumers the option of controlling access to their personal credit data. The service we are developing will let consumers easily lock and unlock access to their Equifax credit files. You will be able to do this at will. It will be reliable, safe and simple. Most significantly, the service will be offered free, for life.

With the extension of the complimentary TrustedID package and free credit freezes into the new year, combined with the introduction of this new service by the end of January, we will be able to offer consumers both short- and long-term support for their personal data security.

> There is no magic cure for data breaches. As we all know, every organization is at risk. When consumers have access to our new service, however, the cybercrime business will become a lot more difficult, and we are committed to doing what we can to help millions of consumers rest easier.

114. Smith later testified before the U.S. House Subcommittee on Digital Commerce and Consumer Protection on October 3, 2017, the U.S. Senate Banking Committee on October 4, 2017, and the U.S. Senate Judiciary Committee on October 4, 2017. During his October 3, 2017 testimony, Smith testified that he would be free to sell shares that would vest at the end of 2017, which U.S. Congressman Greg Walden calculated to be worth about $24 million.

115. On October 3, 2017, Smith testified before the U.S. House Committee on Energy and Commerce's Subcommittee on Digital Commerce and Consumer Protection. In prepared testimony, Smith (i) acknowledged that "the collection of American consumer information and data carries with it enormous responsibility to protect that data"; and (ii) apologized on behalf of the Board, management, and the Company's employees for "not liv[ing] up to that responsibility." Smith claimed the Data Breach was caused by "both human error and technology failures." On multiple occasions during Smith's testimony, Smith blamed an "individual" in Equifax's technology department who had failed to heed security warnings and did not ensure the implementation of software fixes that would have prevented the

breach. Yet Smith had no choice but to also acknowledge that "[a]s CEO I was ultimately responsible for what happened on my watch."

116. During the October 3, 2017 testimony, Smith further testified that a March 8, 2017 alert from U.S.-CERT to Equifax and many other companies was circulated "internally by email" on March 9, 2017, along with a request that IT personnel identify and patch an Apache Struts 2 vulnerability—the software that hackers exploited in the Data Breach and the application that Equifax uses in its online disputes portal. Per Smith, the IT team failed to patch the flaw due to a "communications breakdown," and a scan by Equifax's information security team of the Company's network failed to identify any systems that were vulnerable to the Apache Struts 2 flaw.

117. Smith further testified on October 3, 2017, that he was told about the Data Breach by the Company's CIO on July 31, 2017, following "suspicious activity" being first noticed by "someone in security" on July 29 and July 30, 2017. Smith testified that he was told by the Company's CSO, David Webb, during a face-to-face meeting on July 31, 2017, "that security had noticed a suspicious movement of data out of an environment we call a dispute portal."

118. Smith testified that Equifax Chief Legal Officer John Kelly was responsible for security at Equifax at the time of the Data Breach and its discovery,

and that Kelly reports directly to Smith. Smith testified that Kelly was notified of the "suspicious activity" on July 31, 2017, and that Kelly wrote a "short memo" to Smith regarding the incident. Despite knowledge of the "suspicious activity," Kelly approved the insider sales described herein. Later in his testimony, Smith testified that he "was just informed by staff that the Chief Security Officer [Webb] told the Chief Legal Officer [Kelly] verbally that there was PII that, according to a call with staff yesterday, that actually there was a mention of the breach of personally identifiable information. The CSO [Webb] told—yeah, told us in a call yesterday is what I just heard from staff."

119. Smith testified that the Company hired "leading forensic experts, cyber experts and leading King & Spalding security team" on August 2, 2017. Smith's prepared testimony stated that "[b]y August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables."

120. Smith's prepared testimony stated that on August 15, 2017, Smith "was informed that it appeared likely that consumer PII had been stolen," and he later testified that he was on that date "made aware hackers, kernel hackers got into the system and had PII information." Smith asked for a "detailed briefing" about the

Data Breach on August 15, 2017, and Smith then had a "senior leadership team meeting" with cybersecurity experts and outside counsel on August 17, 2017. Smith testified that at this August 17, 2017 meeting, "the forensic investigation had determined that there were large volumes of consumer data that had been compromised."

121. Smith testified that he notified the "presiding director" of the Board, Mark Feidler, of the Data Breach on August 22, 2017, and the full Board was briefed on August 24, 2017, and August 25, 2017, during "special telephonic board meetings." When asked why Smith waited until August 22, 2017, to notify the Board, Smith testified that the "picture was very fluid. . . . As soon as we thought we had information that was of value to the Board, I reached out to the director [Feidler] on [August 22, 2017], Board meeting on [August 25, 2017], had subsequent Board meetings routinely, if not daily, in some cases as close as last week." Smith testified that the Company began developing remediation plans for consumers on August 24, 2017, and August 25, 2017.

122. Smith testified that on September 1, 2017, Smith convened a Board meeting where the Board discussed the scale of the breach, and by September 4, 2017, Equifax had compiled a list of approximately 143 million consumers whose personal information the Company believed had been stolen.

123. On October 4, 2017, Smith testified before the Senate Committee on Banking, Housing, and Urban Affairs. Senators expressed concern that this tool wouldn't be enough to earn back consumer trust and keep data secure, saying that consumers should be able to ask Equifax to relinquish their data altogether. "This simply is not a company that deserves to be trusted with Americans' personal data," said Senator Sherrod Brown of Ohio. "This breach could have been avoided if you had taken a simple step of administering security patches," added Brown. Senator Elizabeth Warren of Massachusetts stated that companies should have to pay "severe" penalties whenever a consumer's personal data gets stolen. "They didn't have a reason to care to protect our data," Senator Warren lamented, adding, "The incentives in this business are out of whack."

124. Smith also testified before the U.S. Senate Judiciary Committee's Subcommittee on Privacy, Technology & the Law on October 4, 2017, his third session of testimony before Congress. Smith testified that the Data Breach "was made possible by a combination of a human error and a technological error. Human error involved the failure to apply the software patch to our dispute portal in March 2017. The technological error involved a scanner which failed to detect the vulnerability on this particular portal, which had not been patched." Smith testified that on "March 9, [2017,] we took directions to patch, look for and patch that

vulnerability. An individual responsible for the process did not get that request of the right person." Thus, Smith admitted that a mere "individual" was responsible for patching the security systems responsible for protecting the critically sensitive PII stolen as a result of the Data Breach.

125. On October 11, 2017, Professor Jamie Winterton, Director of Strategy at Arizona State University's Global Security Initiative, who testified before the U.S. Senate on October 4, 2017, regarding the Data Breach, submitted[43] the following written response to the U.S. Senate in response to a question from U.S. Senator Christopher Coons of Delaware:

> [Senator Coons:] On March 8, 2017, the Department of Homeland Security alerted Equifax to a software vulnerability. The next day, an Equifax security team was directed to install a routine patch which would solve the vulnerability. That did not occur, and this vulnerability led to the breach, which was not discovered for months. What procedures should be put in place to ensure that adequate cybersecurity does not depend on a chain of communication and execution that may be broken by one person's failure?
>
> [Professor Winterton:] During the hearing, the former CEO of Equifax argued that the breach was in part due to "human error" – that an individual on the security team did not install a patch or communicate clearly which patch should be installed. I disagree. ***This is not an error at the human level, but an error at a leadership and an organizational level. For a single individual to be responsible for Equifax's patch***

[43] Professor Jamie Winterton – Equifax: Continuing to Monitor Data-Broker Cybersecurity Questions for the Record, submitted October 11, 2017, https://www.judiciary.senate.gov/imo/media/doc/Winterton%20Responses%20to%20Coons%20QFRs.pdf (last visited on Jan. 22, 2018).

management shows an institutional lack of concern for security and lack of respect for the people whose data they maintained.

Patching isn't trivial, but it's possibly the most important piece of a company's security posture. Understanding the network is key – which segments can be easily patched, and which have legacy software that may be problematic to update. Those legacy pieces should be isolated from the rest of the network and specifically monitored until an appropriate patch method is identified. Patching speed is key – a 60-day or even 30-day patch cycle often isn't sufficient if an asset may be exposed directly to external attacks, particularly when malicious campaigns or proof-of-concept attacks are known to be exploiting the vulnerability. Some organizations have implemented weekly or daily patching procedures for critical vulnerabilities in exposed systems. The organization's systems should also be subject to regular, consistent monitoring and review – if a patch is available but not installed, that problem should be discovered promptly, elevated, and the risks assessed accordingly. ***Patching isn't just an IT problem; it has organizational-level impacts on compliance as well as operational efficiency – so the patch strategy, with its benefits and risks, should be well understood at the C-suite level.***

126. In its 10-Q filed November 9, 2017, regarding its 3Q17 results (the "3Q17 10-Q"), the Company stated,

ITEM 4. CONTROLS AND PROCEDURES

As discussed in Note 5 of the Notes to the Consolidated Financial Statements in this Form 10-Q, on September 7, 2017, we announced a cybersecurity incident. ***Our review of the circumstances and resulting impact on our internal controls over financial reporting (ICFR) identified two significant deficiencies in our IT General Controls environment, at this point in time.*** As part of the Company's overall plan to address the cybersecurity incident, actions have already been and are being taken in the fourth quarter of 2017 to remediate these significant deficiencies.

> Each of the Company and a Special Committee of the Board of Directors is conducting a review of the cybersecurity incident. We will consider the outcome of this work as we complete our evaluation of ICFR at year-end 2017. As of the end of the period covered by this report, an evaluation was carried out by the Company's management, with the participation of our Interim Chief Executive Officer and Chief Financial Officer, of the effectiveness of our disclosure controls and procedures (as defined in Rule 13a-15(e) under the Securities Exchange Act of 1934). Based upon that evaluation, our Interim Chief Executive Officer and Chief Financial Officer concluded that the disclosure controls and procedures were effective as of the end of the period covered by this report.
>
> In addition, as a result of the review to-date, we have made certain changes to our people, policy and procedures related to ICFR (as defined in Rule 13a-15(f) under the Securities and Exchange Act of 1934), however we do not believe these changes have materially affected or are reasonably likely to materially affect our internal control over financial reporting.

5. The Compensation Packages of Smith, Gamble, Kelley, and Ploder Excluded Legal Fallout From Lax Data Security

127. The Individual Defendants' conscious inaction to known cyberthreats is explained, at least in part, by the Company's executive compensation structure. That structure provides no incentive whatsoever for executives to operate the Company, or to ensure the Company is operated, in a lawful manner. Instead, because the Company's legal expenses and costs are not included, in any way, in the calculation of their compensation, certain executives are free to operate Equifax with impunity, devoid of any risk of personal financial detriment for failing to implement

and/or maintain adequate data security measures or to address known, existing vulnerabilities within the Company's data security controls.

128. Specifically, under Equifax's Annual Incentive Plan ("AIP"), established pursuant to Equifax's 2008 Omnibus Incentive Plan, Equifax's corporate financial performance objectives for named executive officers with Company-wide responsibilities (including Defendants Smith, Gamble, Kelley, and Ploder) were based on "Corporate Adjusted EPS from Continuing Operations" ("Corporate Adjusted EPS"), which is "a non-GAAP financial measure used by the Company for incentive measurement purposes." Corporate Adjusted EPS excludes legal settlements to purportedly "allow[] investors to evaluate our performance for different periods on a more comparable basis." In fourth quarter of 2016 ("4Q16"), for example, Equifax made a $6.5 million adjustment for a settlement with the Consumer Financial Protection Bureau ("CFPB"). In the fourth quarter of 2015, Equifax made an adjustment of $7.9 million for a settlement over software, as well as the same adjustment in the fourth quarter of 2014.

129. For the 2016 Annual Cash Incentive Goal, Corporate Adjusted EPS was weighted at 65% of the Company's incentive performance measures, with the remaining 35% comprised of Corporate Adjusted Operating Revenue from Continuing Operations.

130. On September 13, 2017, an article entitled "Consumers, but Not Executives, May Pay for Equifax Failings" was published in the *New York Times*, and stated the following regarding Equifax's compensation plan:

> Consumers, but Not Executives, May Pay for Equifax Failings
>
> By Gretchen Morgenson
>
> The stunning data breach recently disclosed by Equifax, one of the nation's top three credit reporting agencies, has imperiled millions of consumers, opening them up to identity theft, monetary losses and colossal headaches.
>
> Equifax investors are also shouldering the burden associated with the company's apparently lax security practices. Since disclosing the breach, Equifax's stock has fallen 35 percent, losing its shareholders almost $6 billion in market capitalization.
>
> It remains unclear, though, whether the company's executives will take a financial hit for the failures that allowed thieves to steal Social Security numbers, driver's license numbers and other sensitive data. Indeed, Equifax's top managers may not feel any financial ill effects, given the company's past compensation practices.
>
> Over the last three years, when Equifax determined its top executives' incentive compensation, it has used a performance measure that excluded the costs of legal settlements made by the company. If it follows this practice after dealing with the costs of settling legal claims arising from the security breach, Equifax's top managers will essentially escape financial accountability for the blunder.
>
> This troubles Charles M. Elson, a professor of finance at the University of Delaware and the director of its John L. Weinberg Center for Corporate Governance. "To the investors in the company, the legal settlement does impact earnings and stock price," Mr. Elson said in an interview. "If the shareholders suffer because of this breach, why

should management be excluded? These folks take home all of the upside and want none of the down."

I asked Equifax whether its board would stop excluding legal settlement costs from executive compensation calculations so that management would be required to absorb some of the pain.

An Equifax spokeswoman supplied this statement: "The board is actively engaged in a comprehensive review of every aspect of this cybersecurity incident."

Equifax is not alone in excluding certain costs of doing business from the financial factors it uses to determine executive pay. Such practices have become prevalent among large United States companies.

Equifax uses two main performance measures to decide incentive pay. One, called corporate adjusted earnings per share from continuing operations, is not calculated using generally accepted accounting principles, or GAAP. It is figured by excluding certain costs — such as those related to acquisitions — that normally flow through a company's profit-and-loss statement. This has the effect of making Equifax's earnings per share look better in this measure than they actually do under accounting rules.

Equifax says in regulatory filings that it uses the adjusted earnings figure because it best represents the company's profit growth. Top managers at the company get a larger or smaller annual incentive award based on increases in this measure over the course of a year.

Acquisition expenses make up the bulk of the costs Equifax has excluded from its profit calculation in recent years. But Equifax has also excluded costs associated with impaired investments and legal settlements from the figure.

In regulatory filings, Equifax said its exclusion of legal charges from certain financial results "provides meaningful supplemental information regarding our financial results" and is consistent with the way management reviews and assesses the company's historical performance.

This approach is not unusual. Roughly one-fifth of the companies in the Standard & Poor's 500-stock index excluded legal settlements and fees in their non-GAAP earnings measures in 2016, according to Jack Ciesielski, publisher of The Analyst's Accounting Observer and a close follower of companies' financial reporting.

When settlements are small, of course, excluding the legal costs associated with them is a nonevent. And in recent years that has been the case at Equifax, with settlements equaling around 1 percent of net income.

In the fourth quarter of 2016, for example, Equifax recorded a $6.5 million charge for a settlement with the Consumer Financial Protection Bureau. Under that settlement, which involved deceptive marketing of credit scores to consumers according to the bureau, Equifax paid $3.8 million in restitution to customers, a fine of $2.5 million and $200,000 in legal costs.

But the scope of Equifax's recent security breach is so far-reaching that legal settlements arising from it will most likely be enormous. And this brings up another question: whether Equifax executives should return past pay because of the security failure. Certainly, last year's proxy filings indicate that the pay received by the company's top three executives was based in part on their accomplishments in keeping consumers' data secure.

Consider Richard F. Smith, the chief executive and chairman of the Equifax board, who received $15 million in total compensation in 2016, up from $13 million in 2015. One rationale for his pay package, the proxy said, was Mr. Smith's "distinguished" work in meeting his individual management objectives for 2016. Among those objectives was "employing advanced analytics and technology to help drive client growth, security, efficiency and profitability."

Or take John Gamble, Equifax's chief financial officer. He also received a rating of "distinguished" on his individual objectives, the proxy said, because he continued "to advance and execute global enterprise risk management processes, including directing increased

> investment in data security, disaster recovery and regulatory compliance capabilities." Mr. Gamble received $3.1 million in 2016.
>
> John J. Kelley III, the company's chief legal officer, also achieved a "distinguished" rating from the Equifax board last year. One reason: He continued "to refine and build out the company's global security organization." Mr. Kelley received $2.8 million in compensation last year.
>
> Will these executives be asked to return any of this pay given that their ratings on security are now looking a little less distinguished?
>
> Equifax declined to answer this question.
>
> What the Equifax mess seems to show, yet again, is the heads-I-win, tails-you-lose deal between executives and shareholders that is so prevalent at major corporations today.
>
> As for Equifax's exclusion of litigation costs in its profit measure, Mr. Ciesielski, the accounting expert, said that should be allowed only for events that are outside of management's control. "A hurricane, an earthquake, falling space debris — all those things are exogenous, outside of management's control and ultimately more forgivable," Mr. Ciesielski said. "Bad management leading to customer harm is exogenous and forgivable? That's a lot harder to accept."

131. The Company's 2017 Proxy Statement, filed March 24, 2017, stated the following regarding the Company's incentive compensation:

> **2016 Annual Cash Incentive Goals**
>
> Annual cash incentive awards are designed to reward the achievement of near-term business goals. In addition to financial metrics, annual incentive awards are based on an assessment of individual leadership qualities and contributions toward the achievement of business and strategic goals. When setting the range of performance goals for Corporate Adjusted EPS and Corporate Operating Revenue at the outset of the fiscal year, the Compensation Committee considered our

> financial results from the prior year and our annual operating budget for the coming year. The Committee also considered the history of attainment of goals in prior years, economic and industry conditions, industry sector performance and the views of our shareholders.
>
> The 2016 corporate financial performance objectives for the NEOs with Company-wide responsibilities (Messrs. Smith, Gamble and Kelley and Ms. Rushing) were based on Corporate Adjusted EPS (used to measure profitability) and Corporate Operating Revenue (used to measure top line business growth). The financial objectives for Mr. Ploder, as business unit leader, were focused primarily on relevant business unit revenue and operating income performance (used to measure unit growth and profitability), as well as Corporate Adjusted EPS (to emphasize profitability of the Company as a whole).
>
> *Establishment of Corporate-Level Financial Goals*
>
> The Compensation Committee established corporate financial goals required to earn a cash incentive award for 2016 in a manner that is designed to, within reasonable limits, encourage achievement that exceeds target goals and penalize underachievement, while recognizing the need to encourage performance throughout the year. We set challenging, but realizable, goals, including those that are realizable only as a result of exceptional performance, for the Company and our executives in order to drive the achievement of our short- and long-term objectives.

132. During the August 17 Terry College Speech, Smith admitted that "[f]raud is a huge opportunity for us. It is a massive, growing business for us," he said.

133. In fact, on its November 10, 2017 earnings call with investors discussing third quarter 2017 ("Q3 2017") results, Defendant Gamble described the minimal short-term adverse impact of the Data Breach on the Company's revenues:

> Total revenue for the quarter was $835 million, ***up 4% on a reported basis and up 3% on a local currency basis from Q3 2016***. For the quarter, FX was a $3 million benefit. Adjusted EBITDA margin was 37.4%, up 150 basis points. Adjusted EPS was $1.53, up 6%. In the quarter, we ***estimate*** that the cybersecurity incident negatively impacted total company revenue by 1% to 2% of sales, principally in the U.S.
>
> We have not seen a material negative impact on revenues from the increase in consumers freezing or locking their credit file to date. Prior to the September 7 announcement, approximately 0.5% of Equifax credit files were locked or frozen. Since then, we have seen an increase in volume in the number of locks and freezes placed by consumers, and the total files locked or frozen currently represent about 1.5% to 2% of all Equifax credit files. Approximately 15% to 20% are locks, and the rest are state-filed freezes.

134. Over time, the Data Breach will generate significant additional revenues for the Company. For example, LifeLock controls approximately 27% of the Identity Threat Protection ("ITP") services market, entered in to a four-year agreement, on December 23, 2015, with Equifax to purchase "certain credit products and services from Equifax" that would "comprise a part of LifeLock's identity theft protection services for consumers and include, among others, credit monitoring, credit data and credit score products and services." In a September 2017 interview with Bloomberg Fran Rosch, the Executive Vice President of Consumer Business at Symantec, which acquired Lifelock in February 2017, stated "[w]e're over 100,000 new members and counting since the breach." On a November 1, 2017 Earnings Call, Gregory S. Clark, Symantec's CEO, stated that "Equifax was good,

and it definitely increased member counts in a significant way" and that they "expect it to gain momentum through the remainder of the fiscal year." Thus, as a customer of Equifax, and in the wake of the Data Breach, Lifelock will likely continue to add new members in droves, providing Equifax with increased revenue from its relationship with LifeLock.

135. Intersections Inc. ("Intersections"), who offers ITP services through their Identity Guard product, amended their agreement to "purchase credit information from Equifax" on December 29, 2016, for another five years. In a November 13, 2017 press release announcing financial results for the quarter ended September 30, 2017, Intersections reported that they saw "[s]ubscriber growth late in the third quarter" increasing the Identity Guard subscriber base to "338 thousand subscribers as of September 30, 2017, compared to 329 thousand subscribers as of June 30, 2017," an increase of 9,000 subscribers. The release also stated that looking "ahead to the fourth quarter and 2018," Intersections expected a "strong consumer need for comprehensive identity protection solutions . . ." and that because of the Equifax breach they "stand[] to gain from consumers who want someone other than the credit agencies to protect them." Thus, as a customer of Equifax, and in the wake of the Data Breach, Intersections will likely continue to add new members in droves, providing Equifax with increased revenue from its relationship with Intersections.

136. The Company also offered, as purported restitution, its creditor monitoring service "TrustedID Premier" free of charge for one year. However, the Company's "Frequently Asked Questions" website[44] states (in response to the question, "Will I be automatically enrolled in the new lock service after one year if I am currently enrolled in TrustedID Premier?"), only that, "We will provide additional details prior to rolling out the new service." Thus, the Company may automatically renew and charge customers after the one year of free service expires, further driving revenues for Equifax.

137. Although the Data Breach may be a mere blip in impacting Equifax's revenues and earnings, the mountain of civil, federal, and state liability the Company faces, and the legal costs of such actions, is likely to cost Equifax millions (if not tens of millions or more) dollars for the foreseeable future. However, because the Company's legal expenses and costs are not included, in any way, in the calculation of Smith's, Gamble's, Kelley's, and Ploder's compensation packages, Equifax will be left to bear the brunt of these mountainous expenses alone, while these Defendants sit back and profit from the corporate trauma they helped cause.

[44] https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last accessed Jan. 9, 2018).

D. The Individual Defendants Were Obligated to Safeguard the Company's Interests and Comply with Applicable Laws

1. General Duties

138. By reason of their positions as officers, directors, and/or fiduciaries of Equifax, and because of their ability to control the business and corporate affairs of Equifax, the Individual Defendants owed, and owe, the Company and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were, and are, required to use their utmost ability to control and manage Equifax in a fair, just, honest, and equitable manner. The Individual Defendants were, and are, required to act in furtherance of the best interests of Equifax and its shareholders so as to benefit all shareholders equally, and not in furtherance of their personal interest or benefit.

139. Each director and officer of the Company owed, and owes, to Equifax and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

140. To discharge their duties, the officers and directors of Equifax were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial affairs of the Company. By virtue

of such duties, the officers and directors of Equifax were required to, among other things:

(a) ensure that the Company complied with its legal obligations and requirements, including acting only within the scope of its legal authority and disseminating truthful and accurate statements to the investing public;

(b) conduct the affairs of the Company in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, avoid wasting the Company's assets, and maximize the value of the Company's stock;

(c) properly and accurately guide shareholders and analysts as to the true financial and business prospects of the Company at any given time, including making accurate statements about the Company's business practices, operations, financials, compliance policies and practices, and internal controls;

(d) remain informed as to how Equifax conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiry in connection therewith, and take steps to correct such conditions or practices and make such disclosures as necessary to comply with federal, state, and municipal laws, rules, and regulations; and

(e) ensure that Equifax was operated in a diligent, honest, and prudent manner in compliance with all applicable laws, rules, and regulations.

141. Boards of directors are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs. Boards are responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs.

142. Directors should, instead, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization.

143. Boards should establish that the CEO and the senior executives are fully engaged in risk management, and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, boards can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business, nor a mere

supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.

144. Boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Cyber-risk must be considered as part of a board's overall risk oversight. In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats.

145. While there is no "one-size-fits-all" way to properly prepare for the various ways a cyber-attack can unfold, and what responses may be appropriate, an ill-thought-out response can be far more damaging than the attack itself. Boards should prepare for worst-case scenario cybersecurity breaches and help management develop immediate response plans, including public disclosure procedures and economic recovery strategies, to mitigate potential damages. These plans should include, among other things, whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and to investors).

146. Adam Brand, a director in global consulting firm Protiviti's IT Security & Compliance practice, has stated, "I would expect more of companies with

advanced security programs, or those who focus on data as a business. They should be detecting intrusions in days not months."[45]

147. On June 10, 2014, then-SEC Commissioner Luis A. Aguilar gave a speech entitled "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus"[46] before the "Cyber Risks and the Board" Conference in New York City. Commissioner Aguilar stated the following regarding duties owed by boards of directors:

> Effective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets.
>
> * * *
>
> But management without accountability can lead to self-interested decision-making that may not benefit the company or its shareholders. As a result, shareholders elect a board of directors to represent their interests, and, in turn, the board of directors, through effective corporate governance, makes sure that management effectively serves the corporation and its shareholders.
>
> * * *

[45] *Equifax auditors are on the hook for data security risk controls*, Market Watch, https://www.marketwatch.com/story/equifax-auditors-are-on-the-hook-for-data-security-risk-controls-2017-10-02 (last visited Jan. 10, 2018).

[46] Commissioner Luis A. Aguilar, *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*, https://www.sec.gov/news/speech/2014-spch061014laa (last visited Jan. 10, 2018).

Although primary responsibility for risk management has historically belonged to management, the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs.

* * *

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight.

* * *

Another way that has been identified to help curtail the knowledge gap and focus director attention on known cyber-risks is to create a separate enterprise risk committee on the board. It is believed that such committees can foster a "big picture" approach to company-wide risk that not only may result in improved risk reporting and monitoring for both management and the board, but also can provide a greater focus — at the board level — on the adequacy of resources and overall support provided to company executives responsible for risk management.

* * *

At a minimum, boards should have a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices.

* * *

Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event.

148. Boards of directors are responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs. *See, e.g.*, Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 Iowa J. Corp. L. 967 (2009) ("Although primary responsibility for risk management rests with the corporation's top management team, the board of directors is responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs.").

149. Directors should, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall

compliance program, but is instead an integral component of strategy, culture and business operations. *See* Martin Lipton, *Risk Management and the Board of Directors–An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (2014).[47]

150. Indeed, given (i) the centrality of PII to Equifax's core business, and (ii) the critically sensitive PII held by Equifax, the Individual Defendants were obligated to develop, implement, and maintain the very best data security systems, controls, and safeguards available. This includes developing, implementing, and maintaining an action plan for responding to a data breach ***before*** a data breach occurs, including outlining employee and Board responsibilities, who should be contacted and when, how the Company would communicate to the public, and how the breach would be assessed.

2. Duties Under Georgia Law

151. As officers and directors of a Georgia corporation, Equifax's officers and directors were required to "discharge [their] duties . . . in good faith . . . and [w]ith the care an ordinarily prudent person in a like position would exercise under

[47] http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014 (last visited Jan. 10, 2018).

similar circumstances." O.C.G.A. §§ 14-2-830(a)(1), (2) (directors) and 14-2-842(a)(1), (2) (officers).

152. Pursuant to the Georgia Security Breach Notification Act, O.C.G.A. §§ 10-1-912, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system (that was reasonably likely to have caused unauthorized persons to acquire PII) ***in the most expedient time possible and without unreasonable delay***.

153. Pursuant to O.C.G.A. § 51-1-6, "[w]hen the law requires a person to perform an act for the benefit of another or to refrain from doing an act which may injure another, although no cause of action is given in express terms, the injured party may recover for the breach of such legal duty if he suffers damage thereby."

3. Duties Under Federal Laws

154. The Individual Defendants had a duty to promptly disseminate accurate and truthful information with regard to the Company's business practices, operations, financials, compliance policies and practices, and internal controls so that the market price of the Company's stock would be based on truthful and accurate information. The Individual Defendants were further obligated to prevent insiders from selling stock during a time of wait before the announcement a cybersecurity failure.

155. An EY publication entitled "2016 SEC annual reports – Form 10-K"[48] regarding SEC disclosures, published in November 2016, reminds its clients and potential clients that existing disclosure rules are applicable to "cybersecurity risks and incidents that could have a material effect on a registrant's financial statements." The report also notes that the SEC's guidance requires material cybersecurity risks or cyber incidents to be disclosed "when necessary to make other required disclosures, in light of the circumstances, not misleading."

156. In the SEC's Risk Alert published August 7, 2017, entitled "Observations From Cybersecurity Examination"[49] by the Office of Compliance Inspections and Examinations ("OCIE") regarding recent exams of registered investment advisors and funds, the SEC identified consistent deficiencies by various regulated entities, which are also applicable to any public company, including: (i) failures to reasonably tailor policies and procedures; (ii) failures to adhere to or enforce policies and procedures; (iii) failures to adequately conduct system

[48] http://www.ey.com/Publication/vwLUAssets/SECAnnualReports10K_03265-161US_17November2016/$FILE/SECAnnualReports10K_03265-161US_17November2016.pdf (last visited Jan. 9, 2018).

[49] https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf (last visited Jan. 10, 2018).

maintenance, resulting in Regulation S-P issues; and (iv) failure to remediate high-risk observations discovered through penetration tests and vulnerability scans.

157. In connection with the August 7, 2017 OCIE Risk Alert, the SEC recommended the following best practices, which also serve as best practices for any public company: (i) maintenance of an inventory of data, information, and vendors; (ii) classification of risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor; (iii) detailed cybersecurity-related instructions for issues such as penetration tests, security monitoring/auditing, access rights, and reporting guidelines for lost, stolen, or unintentionally disclosed sensitive information; (iv) maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, including patch management policies; (v) established and enforced controls for access to data and systems; (vi) mandatory employee training at onboarding and periodically thereafter; and (vii) engaged senior management.

158. The Financial Services Modernization Act of 1999, or Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et. seq.*, ("GLBA"), regulates, among other things, the use of non-public, personal information of consumers that is held by financial institutions. The GLBA provides that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the

privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a). Specifically, Equifax is subject to various GLBA provisions, including rules relating to (i) the use or disclosure of the underlying data, and (ii) the physical, administrative, and technological protection of non-public, personal, financial information. The GLBA defines "nonpublic personal information" as personally identifiable financial information "(i) provided by the consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." *Id.* at § 6809(4)(A). Breach of the GLBA can result in civil and/or criminal liability, and sanctions by regulatory. authorities, including fines of up to $100,000 per violation and up to five years' imprisonment for individuals. Regulatory enforcement of the GLBA is under the purview of the U.S. Federal Trade Commission ("FTC"), the federal prudential banking regulators, the SEC, and state attorney generals, acting alone and/or in concert with each other.

159. Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies. Pursuant to the FTC Act, the Individual

Defendants were required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal and financial information in Equifax's possession from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons.

160. Equifax is also subject to the Fair Credit Reporting Act ("FCRA") and other federal and foreign laws regulating the use and protection of sensitive data.

4. Duties Under the Laws of Other States

161. Pursuant to the Alaska Personal Information Protection Act, Alaska Stat. §§ 45.48.010, *et seq.*, the Individual Defendants were required to (i) accurately notify effected Alaskans if they become aware of a breach of Equifax's data security system in the most expedient time possible and without unreasonable delay, (ii) determine the scope of the breach and restore the reasonable integrity of the information system, and (iii) disclose the Data Breach in a timely and accurate fashion.

162. Pursuant to the California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, the Individual Defendants were required to notify California residents when their PII has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay" (Cal. Civ. Code § 1798.82) and

include "the types of personal information that were or are reasonably believed to have been the subject of the breach." (*Id.*)

163. Pursuant to the Colorado Security Breach Notification Act, Colo. Rev. Stat. Ann. §§ 6-1-716, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system in the most expedient time possible and without unreasonable delay.

164. Pursuant to the Delaware Computer Security Breach Act, 6 Del. Code Ann. §§ 12B-102, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system (which is reasonably likely to result in the misuse of a Delaware resident's PII) in the most expedient time possible and without unreasonable delay.

165. Pursuant to the District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system in the most expedient time possible and without unreasonable delay.

166. Pursuant to the Hawaii Security Breach Notification Act, Haw. Rev. Stat. §§ 487N-1, *et seq.*, the Individual Defendants were required to accurately notify

affected persons if they became aware of a breach of Equifax's data security system without unreasonable delay.

167. Pursuant to the Personal Information Security Breach Protection Law, Iowa Code Ann. §§ 715C.2, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system in the most expeditious time possible and without unreasonable delay.

168. Pursuant to Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system (that was reasonably likely to have caused misuse of PII) in the most expedient time possible and without unreasonable delay.

169. Pursuant to the Kentucky Computer Security Breach Notification Act, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system (that was reasonably likely to have caused unauthorized persons to acquire PII) in the most expedient time possible and without unreasonable delay.

170. Pursuant to La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware

of a breach of Equifax's data security system (that was reasonably likely to have caused unauthorized persons to acquire PII) in the most expedient time possible and without unreasonable delay.

171. Pursuant to the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq.*, the Individual Defendants were required to (i) "protect personal information from unauthorized access, use, modification, or disclosure" (Md. Comm. Code § 14-3503(a)), (ii) "implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed," (iii) when they discover or are "notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that PII . . . has been or will be misused as a result of the breach." (Md. Comm. Code § 14-3504(b)(1)), and (iv) "[i]f, after the investigation is concluded . . . determine[] that misuse of . . . PII has occurred or is reasonably likely to occur as a result of a breach of the security system . . . shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical."

172. Pursuant to the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72, *et seq.*, the Individual Defendants were required to accurately notify affected persons if they discover a security breach, or receive notice of a

security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay.

173. Pursuant to N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware of a breach of Equifax's data security system (in which misuse of PII has occurred or is reasonably likely to occur) as soon as possible.

174. Pursuant to the New Jersey Customer Security Breach Disclosure Act, N.J. Stat. Ann. §§ 56:8-163, *et seq.*, the Individual Defendants were required to notify "New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person." (N.J. Stat. Ann. § 56:8-163(b)).

175. Pursuant to the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. Art. 2A §§ 75-60, *et seq.*, the Individual Defendants were required to accurately notify affected persons if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay.

176. Pursuant to the Oregon Consumer Identity Theft Protection Act, Or. Rev. Stat. Ann. §§ 646A.604(1), *et seq.*, the Individual Defendants were required to

"implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure" (Or. Rev. Stat. Ann. § 646A.622(1)) and accurately notify if they become aware of a breach of Equifax's data security system in the most expeditious time possible and without unreasonable delay.

177. Pursuant to the South Carolina Data Breach Security Act, S.C. Code Ann. §§ 39-1-90, *et seq.*, the Individual Defendants were required to accurately notify affected persons following discovery or notification of a breach of Equifax's data security system (if personal information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm) in the most expedient time possible and without unreasonable delay.

178. Pursuant to the Tennessee Personal Consumer Information Release Act, Tenn. Code Ann. §§ 47-18-2107, *et seq.*, the Individual Defendants were required to accurately notify affected persons following discovery or notification of a breach of Equifax's data security system (in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person) in the most expedient time possible and without unreasonable delay.

179. Pursuant to the Virginia Personal Information Breach Notification Act, Va. Code. Ann. §§ 18.2-186.6, *et seq.*, the Individual Defendants were required to accurately notify affected persons following discovery or notification of a breach of Equifax's data security system (if unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay.

180. Pursuant to the Washington Data Breach Notice Act, Wash. Rev. Code Ann. §§ 19.255.010, *et seq.*, the Individual Defendants were required to accurately notify affected persons following discovery or notification of the breach of Equifax's data security system (if PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured) in the most expedient time possible and without unreasonable delay.

181. Pursuant to Wis. Stat. Ann. §§ 134.98(2), *et seq.*, the Individual Defendants were required to accurately notify affected persons if they knew that PII in Equifax's possession has been acquired by a person whom it has not authorized to acquire the PII within a reasonable time.

182. Pursuant to Wyo. Stat. Ann. §§ 40-12-502(A), *et seq.*, the Individual Defendants were required to accurately notify affected persons if they became aware

of a breach of Equifax's data security system (if the misuse of personal identifying information has occurred or is reasonably likely to occur) in the most expedient time possible and without unreasonable delay.

5. The Board's Committees Were Obligated to Oversee and Monitor Equifax's Data Security Oversight Systems and Controls

a. Audit Committee Duties

183. Aside from those duties described above in §§ IV.D.1–4, *supra*, which are applicable to all directors and executives, the members of the Audit Committee owed additional, specific duties to Equifax, under the Audit Committee's Charter, to ensure:

> (1) the integrity of the Company's statements and other financial information provided to any governmental body, its shareholders or the public; (2) the Company's systems for complying with legal and regulatory requirements; . . . and (5) the integrity of the Company's internal controls regarding finance, accounting, and auditing, and its financial reporting processes.

184. Specifically, according to Equifax's Audit Committee Charter, the Audit Committee's specific duties and responsibilities include the following:

> **A. <u>Financial Statements Review</u>**
>
> 1. Review the audited financial statements, the Management's Discussion and Analysis section and other material financial content of the Company's annual report to shareholders and annual report on Form 10-K, and discuss with management and the independent auditors prior to publication of the annual report to shareholders and the filing of the Company's Form 10-K.

2. Review the unaudited financial statements, the Management's Discussion and Analysis section and other material financial content of each quarterly report on Form 10-Q and discuss with management and the independent auditors prior to filing the Form 10-Q. To the extent permissible under NYSE Rules, the Committee may delegate this review to the Chair or another member.

3. Review and comment concerning earnings press releases and financial information and earnings guidance provided to analysts and rating agencies prior to the release or dissemination of such information. In lieu of reviewing each such disclosure prior to release or dissemination, the Committee may discuss generally with management the types of information to be disclosed and the types of presentation to be made, and establish policies or guidelines for such disclosures. To the extent permissible under NYSE Rules, the Committee may delegate this review to the Chair or another member.

4. Prepare the annual Audit Committee report for inclusion in the Company's proxy statement, in accordance with all applicable rules and regulations.

* * *

D. <u>Financial Reporting and Auditing</u>

1. Review with the Company's principal executive and financial officers, internal auditors and independent auditors the integrity of the Company's financial reporting processes, including (a) disclosures made to the Committee by the Company's CEO and CFO during their certification process for the Form 10-K and Forms 10-Q about any significant deficiencies in the design or operation of internal controls or material weaknesses therein and any fraud, whether or not material, that involves management or other employees who have a significant role in the Company's internal controls; and (b) assurance from the independent auditors that Section 10A(b) of the Securities Exchange Act of 1934 has not been implicated. Section 10A(b) relates to illegal

acts that have come to the attention of the independent auditors during the course of the audit.

2. Review with the independent auditors, the internal auditors and management, the adequacy and effectiveness of the Company's internal control over financial reporting, disclosure controls and procedures and the completeness and accuracy of the Company's financial statements and financial reporting process. The Committee shall consider the quality of presentation of, among other matters, critical accounting policies, off-balance sheet transactions and financial measures presented on a basis other than in accordance with generally accepted accounting principles.

3. In consultation with the independent auditors, management and the Company's internal audit department, review all major changes and improvements pertaining to the Company's financial and accounting principles, practices, internal control over financial reporting and disclosure controls and procedures.

4. Establish regular and separate systems of reporting to the Committee by the independent auditors and the internal auditors regarding any significant judgments made in management's preparation of the financial statements and the view of each as to the appropriateness of any such judgments.

5. Discuss, either as a Committee or through its Chair (or designee), with the independent auditors, the internal auditors and management the results of the independent accountants' review of the interim financial information prior to the filing of the quarterly Form 10-Q with the SEC, to the extent required by generally accepted auditing standards.

6. Discuss with the independent auditors and management the scope, planning and staffing of the annual audit prior to the commencement of the audit.

7. Obtain and review at least annually within 90 days prior to the filing of the Company's annual report on Form 10-K a report or

report update from the independent auditors setting forth: all critical accounting policies and practices to be used in the financial statements; all alternative treatments within generally accepted accounting principles for policies and practices related to material items that have been discussed with management, including the ramifications of the use of such alternative disclosures and treatments and the treatment preferred by the independent auditors; and any other material communications between the independent auditors and management, such as any management letter or schedule of unadjusted differences.

8. After the annual audit, review with the independent auditors and the internal audit department the matters required under Statement of Auditing Standards Nos. 61 and 90 or other applicable accounting standards or rules of the PCAOB, any significant difficulties encountered during the course of the audit, including any restrictions on the scope of work or access to required information and any significant unresolved disagreements with management. The Committee shall review with the independent auditor any audit problems or difficulties and management's response, and shall resolve any disagreements between management and the independent auditors.

E. <u>Ethical and Legal Compliance</u>

1. Ensure the Company maintains an appropriate code of conduct and business ethics compliance program and perform an annual review of its effectiveness. Review requests for and determine whether to grant or deny waivers of the Company's ethics code(s) applicable to directors and executive officers.

2. Exercise oversight with respect to the structure, operation and efficacy of the Company's regulatory compliance program. This oversight will include:

   a. regular review of legal, tax and regulatory matters that may have a material impact on the Company's financial statements and disclosures

b. regular review of compliance with applicable laws and regulations

c. approval of the annual compliance audit plan and review of such audits to be performed by the Internal Audit department of the Company; and

d. review of significant inquiries received from regulators or government agencies, including, without limitation, issues pertaining to federal or state securities or consumer financial protection laws or regulations or enforcement or other actions brought or threatened to be brought against the Company by, regulators or government agencies.

3. At least once a year, review and discuss with management the Company's policies with respect to risk assessment and risk management, including, without limitation, material regulatory, compliance and litigation risks facing the Company. Without limiting the generality of the foregoing, such reviews and discussions will include the implications of the Company's internal use of its data sets on consumers civil rights and the potential impact of such issues on the Company's business, operations and management. The Committee will direct management to take appropriate steps to monitor and mitigate such exposures and policy concerns.

4. Establish procedures as required by law for the receipt, retention and treatment of complaints on accounting, internal accounting controls or auditing matters, as well as for confidential, anonymous submissions by Company employees of concerns regarding questionable accounting or auditing matters.

185. The Company's Audit Committee Charter was in effect at all times during the Relevant Period and, thus, imposed the duties set forth above on the Audit Committee Defendants.

b. Duties Pursuant to the Technology Committee Charter

186. Aside from those duties described above in §§ IV.D.1–4, *supra*, which are applicable to all directors and executives, the members of the Technology Committee owed additional, specific duties to Equifax, under the Technology Committee's Charter, to:

> [R]eview and monitor the Company's technology strategy and significant technology investments in support of its evolving global business needs. Areas of review include: information technology strategy; significant new product lines or technology investments; and ***the Company's response to external technology-based threats*** and opportunities. ***In addition, the Committee will oversee the Company's mitigation of any identified enterprise-wide risks in the above areas***.

187. Specifically, according to Equifax's Technology Committee Charter, the Technology Committee's duties and responsibilities include the following:

> The goals and responsibilities of the Committee are to monitor the Company's long-term strategy and significant investments in the areas listed below. The Committee may conduct its review of any such policy or program as the Committee Chair shall determine. The intervals for review of any given policy or program may be annual, biannual, or at longer or shorter intervals, depending upon the nature of the subject matter and developments affecting the Company with respect to that subject matter.
>
> 1. Information technology long-term strategy in support of the Company's evolving global business needs.
>
> 2. Review and present observations to the Board with respect to the annual technology budget.
>
> 3. Significant new product development programs (including software initiatives) and new technology investments, including

technical and market risks associated with product development and investment.

4. Future trends in technology that may affect the Company's strategic plans, including overall industry trends and new opportunities and threats occasioned by new technologies, especially disruptive technologies.

5. ***Review the Company's technology investments and infrastructure associated with risk management, including policies relating to information security, disaster recovery and business continuity***.

6. Assess the scope and quality of the Company's intellectual property.

7. Undertake from time to time such additional activities within the scope of the Committee's primary purposes as it may deem appropriate and/or as assigned by the Board of Directors, the Chairman of the Board and Chief Executive Officer.

188. Upon information and belief, the Company maintained a Technology Committee Charter during the Relevant Period that imposed the same, or substantially and materially the same or similar, duties on the Technology Committee Defendants as those set forth above.

c. Duties Pursuant to the Compensation Committee Charter

189. Aside from those duties described above at §§I V.D.1–4, *supra*, which are applicable to all directors and executives, the members of the Compensation Committee owed additional, specific duties to Equifax under the Compensation Committee's Charter to:

> [A]ssist the Board [] of Directors [] in fulfilling its oversight responsibility with respect to (A) determining and evaluating the compensation of the Chief Executive Officer []; (B) approving and monitoring the executive compensation plans, policies and programs of the Company; (C) reviewing and discussing with the Company's management the Compensation Disclosure and Analysis "CD&A" to be included in the Company's annual proxy statement and determine whether to recommend to the Board that the CD&A be included in the proxy statement; and (D) advising management on succession planning and other significant human resources matters.

190. Specifically, according to Equifax's Compensation Committee Charter, the Compensation Committee's specific duties and responsibilities include the following:

> **A. <u>Executive Compensation Matters</u>**
>
> 1. Review and approve corporate goals and objectives relevant to compensation of the CEO. The Committee shall evaluate the CEO's performance in light of these goals and objectives and shall determine and set the CEO's compensation level based on such evaluation.
>
> 2. Oversee the evaluation of and make determinations regarding compensation for all other executive officers and any other corporate officers who are subject to the provisions of Section 16 of the Exchange Act (or any successor rule(s) to the same effect) (the "Section 16 Officers").
>
> 3. In determining or recommending the long-term incentive component of CEO and Section 16 Officer compensation, the Committee will generally consider the Company's performance and relative shareholder return, the value of similar incentive awards to the CEO and other Section 16 Officers at comparable companies, and the awards given to the Company's CEO and Section 16 Officers in past years.

4. Authorize and approve any employment, severance, change-in-control or similar termination agreement, award or payment proposed to be made with or to any current or former Section 16 Officer.

5. Approve equity compensation awards for the CEO and other Section 16 Officers.

6. Determine the Company's policy with respect to the application of Code Section 162(m), and the deductibility of executive compensation for federal income tax purposes. The Committee will approve goals and awards under the compensation plans of the Company as required by Section 162(m).

7. Prepare a report annually on executive compensation for inclusion in the Company's proxy statement, in accordance with all applicable rules and regulations.

8. The Committee may delegate responsibility for the day-to-day management of the Company's executive compensation programs.

9. Conduct an annual risk assessment of the Company's compensation programs.

B. <u>Plan Matters</u>

1. Create, authorize, approve, amend and/or terminate any new or existing executive officer and employee compensation and benefit plans.

2. Determine and set the Company's discretionary matching contributions to the Company's 401(k) Plan (the "Plan") and take any other actions required of it under the Plan.

3. Appoint the members of the Company's Group Plans Administrative Committee (the "Administrative Committee") whose members shall be responsible for oversight and administrative duties regarding the plans as determined by the Committee.

4. Annually receive a presentation regarding the effectiveness and funded status of the Company's compensation and qualified benefit plans from the Group Plans Administrative Committee.

191. The Company's Compensation Committee Charter was last revised effective May 2, 2013, and, thus, imposed the duties set forth above on all Compensation Committee Defendants at all times during the Relevant Period.

d. Duties Pursuant to the Company's Code of Ethics and Business Conduct

192. Additionally, the Individual Defendants, as officers and/or directors of Equifax, were, and are, bound by the Company's Code of Ethics and Business Conduct (the "Code") which, "provides information about our personal responsibilities, including complying with the law and applying our good judgment each and every day," among other things. All of Equifax's employees, officers, and directors are expressly bound to abide by the Code.

193. According to the Code, "no reason, including the desire to meet business goals, should ever be an excuse for violating laws, regulations, the Code or Equifax policies."

194. The Code explains in great detail the paramount nature of protecting personal information, and the Company's legal requirement to do so. For example, the Code states:

> In recent years, individuals, companies and governments have grown increasingly concerned about the privacy and security of personal information. As a result, laws protecting personal information and how it may be collected, shared, and used are becoming more common.
>
> Many of us have access to personal information related to our colleagues and others. While protecting this information may now be a legal requirement, for us at Equifax privacy has always been necessary.
>
> **MAKE SURE YOU:**
>
> * * *
>
> Protect the confidentiality of personal information of current and former colleagues, as well as job applicants, business partners and customers.

The Code then specifically addresses "Protecting the Privacy and Confidential Information of Others," noting that "[o]ur customers and our business partners place their trust in us. We must protect their confidential information." To that end, the Code requires that all employees, officers and directors:

> Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access).

Additionally, the Code provides: "One of our most valuable assets is information. Each of us must be vigilant and protect confidential information. This means keeping it secure . . . ."

195. With respect to "Honest and Fair Dealing," the Code provides:

> Equifax officers, directors and employees must deal fairly with the Company's customers, suppliers, business partners and competitors. Always tell the truth about our services and capabilities and never make promises we can't keep. Do not take unfair advantage through manipulation, concealment, abuse of privileged or confidential information, misrepresentation, fraudulent behavior, or any other unfair practice. In short, always apply the same ethical principles, of respect and teamwork, as if the partners were fellow employees.

Accordingly, the Code requires that all employees, officers, and directors "[a]lways make business decisions in the best interest of Equifax."

196. The Code also addresses the need to keep accurate books and records, and make accurate and complete public disclosures, as follows:

> Business partners, government officials and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the Company so that we can make good decisions.
>
> Our books and records must be clear, complete and in compliance with accepted accounting rules and controls. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate and complete and maintained in a manner that is consistent with our system of internal controls.
>
> If you suspect any irregularity relating to the integrity of our records, you need to report it immediately to your supervisor, the Legal Department or the Corporate Ethics Officer.

197. The Code strictly prohibits insider trading, providing:

Insider Trading and "Tipping" Prohibited

No Equifax employee, officer, director or other "insider" may purchase or sell Equifax securities while in possession of material, nonpublic information relating to Equifax ("insider trading"). In addition, no Equifax employee, officer, director or other insider may disclose material, nonpublic information about Equifax, or any other company with which Equifax deals, to others ("tipping"), unless authorized to do so.

Additional Trading Restrictions May Apply

In addition to the general prohibitions against insider trading and tipping, certain insiders with regular access to material, nonpublic information may only trade in Equifax securities during specified trading windows and/or pursuant to pre-clearance and reporting requirements. You will be notified by the Office of Corporate Secretary if you are subject to these additional restrictions.

Covered Insiders

The concept of "insider" is broad. It includes all Equifax employees, officers and directors, as well as their family members and other related parties. It also includes other persons (including consultants, accountants, legal counsel and other advisors) who are not employed by Equifax but who have access to material, nonpublic information about the Company.

Insider Trading is a Serious Crime

The penalties for insider trading or tipping are severe, both for the individuals involved in the unlawful conduct and their employers. Where a violation occurs, a person can be subject to substantial penalties, including criminal liability, civil liability and disciplinary action (up to termination of employment).

Material, Nonpublic Information

Information is considered "material" if:

> a reasonable investor would consider the information important in making a decision of whether to buy, hold or sell a security;
>
> a reasonable investor would view the information as significantly altering the total mix of information in the marketplace about the company that issued the security; or
>
> the information could reasonably be expected to have a substantial effect (positive or negative) on the price of the security.
>
> * * *
>
> **MAKE SURE YOU:**
>
> * * *
>
> Do not buy or sell, or advise anyone else to buy or sell, the securities of Equifax (or such other company) if you are in possession of material, nonpublic information regarding Equifax (or material, nonpublic information regarding any other publicly-traded company that you have obtained as a result of your employment with Equifax), until that information has been publicly disclosed.

198. Upon information and belief, the Company maintained a version of the Code during the Relevant Period that imposed the same, or substantially and materially the same or similar, duties on, among others, the Individual Defendants, as those set forth above.

V. THE DIRECTOR DEFENDANTS VIOLATED SECTION 14(A) OF THE EXCHANGE ACT AND SEC RULE 14A-9, AND BREACHED THEIR FIDUCIARY DUTIES, BY CAUSING THE COMPANY TO FILE A MATERIALLY MISLEADING PROXY STATEMENT

199. On March 24, 2017, the Director Defendants caused Equifax to file a proxy statement for its 2017 annual meeting of shareholders pursuant to

Section 14(a) of the Exchange Act (the "2017 Proxy Statement"). In the 2017 Proxy Statement, the Director Defendants solicited shareholder votes to re-elect 11 director nominees to the Board, including Defendants Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Smith, Stock, and Templeton. However, the 2017 Proxy Statement contained materially false and misleading statements with respect to this vote. For example, the 2017 Proxy Statement represented the following with respect to various committees of the Board: (i) that the Audit Committee "[r]eviews our policies related to enterprise risk assessment and risk management"; (ii) that the Compensation Committee "[c]onducts an annual risk assessment of our compensation programs"; and (iii) that the Technology Committee "[o]versees the execution of technology strategies formulated by management and technology risk and opportunities," and "[p]rovides guidance on technology as it may pertain to . . . security concerns."

200. The 2017 Proxy Statement also detailed the following concerning the Board's role in risk management and oversight:

> **How We Manage Risk**
>
> We have a rigorous enterprise-wide risk management ("ERM") program targeting controls over operational, financial, legal and regulatory compliance, reputational, technology, privacy, data security, strategic and other risks that could adversely affect our business. The program also includes crisis management, disaster recovery and business continuity planning. Our ERM program is designed to support

the achievement of our organizational and strategic objectives, to identify and manage risks, to improve long-term organizational performance and to enhance shareholder value. The implementation and execution of our ERM program is supervised by the director of our internal audit department.

Each business unit and corporate support unit has primary responsibility for assessing and mitigating risks within its respective areas of responsibility. Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from the director of our internal audit department. In addition, our director of internal audit reports to the Audit Committee on a quarterly basis and reports annually to the full Board, as described below under "Board Risk Oversight."

Board Risk Oversight

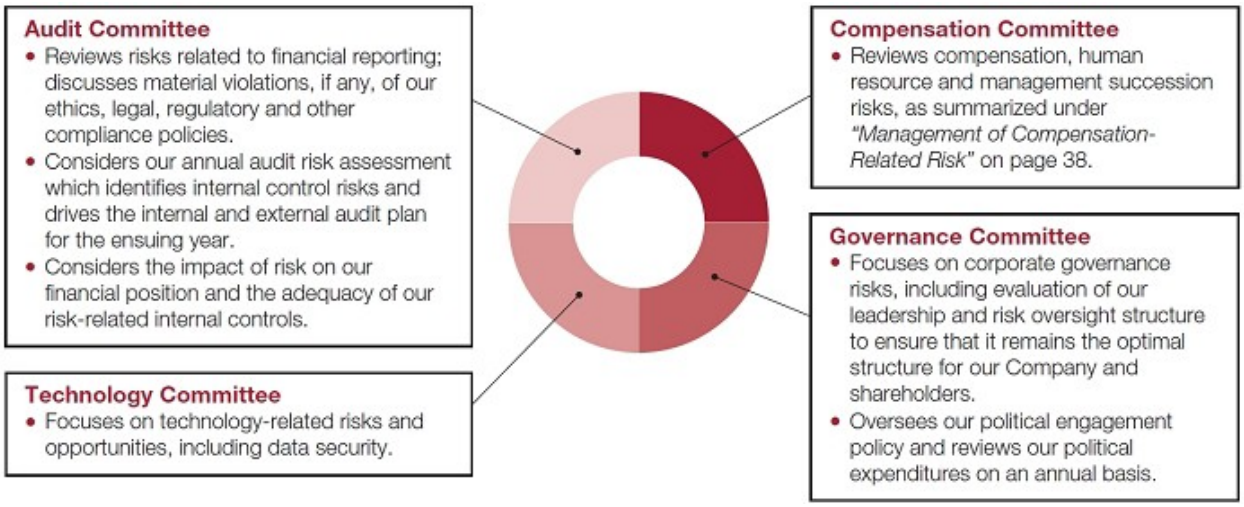
Our Board oversees risk management at the Company. The Board exercises direct oversight of strategic risks to the Company and other risk areas not delegated to one of its committees.

The risk management roles and responsibilities of the Board and its committees are:

Board of Directors

- Monitors our "tone at the top" and risk culture and oversees emerging strategic risks.
- On an annual basis, the Board performs an enterprise risk assessment with management to review the principal risks facing the Company and monitors the steps management is taking to map and mitigate these risks.
    - The Board then sets the general level of risk appropriate for the Company through business strategy reviews.
    - Risks are assessed throughout the business, focusing on (i) financial, operational and strategic risk, and (ii) ethical,

legal, privacy, data security (including cybersecurity), regulatory and other compliance risks.



201. The 2017 Proxy Statement noted that Defendant Smith received $3,045,000 in incentives in 2016 for purportedly meeting certain performance requirements, including $1,979,250 for meeting his Corporate Adjusted EPS target, $456,750 for meeting his "Corporate Operating Revenue" target, and $609,000 for meeting his "Individual Objectives" target. In support of Smith purportedly meeting his performance targets, the 2017 Proxy Statement notes that Smith achieved a rating of "Distinguished" on the following individual objectives for 2016:

- Executing the Company's strategy of diversifying and deepening product offerings to improve financial performance in all the business units in a highly challenging global business environment, generating the strong financial results previously noted in this CD&A.

- Leading the Company's efforts to continue strategically building and rebalancing its capabilities with high value acquisitions, including expanding the Company's geographic reach into Australia, New

Zealand and other markets through the acquisition of the Veda Group Limited in February 2016.

- Refining and executing the Company's long-term Growth Playbook strategy by expanding our role in client business decisions and processes through product innovation and delivering unique value to the customer.

- Employing advanced analytics and technology to help drive client growth, security, efficiency and profitability.

- Investing in emerging opportunities and international expansion.

- Diversifying data sources and products.

- Maximizing the use of analytics and decisioning technology to differentiate the Company's product offerings.

- Implementing measures to control expense growth in line with revenue growth; driving operational efficiencies through LEAN and other continuous business process improvements.

- Driving a performance-driven culture to deliver sustained long-term business growth; retaining and developing a strong leadership team; and demonstrating exemplary leadership and values.

202. The 2017 Proxy Statement also noted that Defendant Gamble received $758,692 in incentives in 2016 for purportedly meeting certain performance targets, including $493,150 for meeting his Corporate Adjusted EPS target, $113,804 for meeting his "Corporate Operating Revenue" target, and $151,738 for meeting his "Individual Objectives" target. In support of Gamble purportedly meeting his performance targets, the 2017 Proxy Statement notes that Gamble achieved a rating of "Distinguished" on the following individual objectives for 2016: "Continuing to

advance and execute global enterprise risk management processes, including directing increased investment in data security, disaster recovery and regulatory compliance capabilities."

203. The 2017 Proxy Statement also noted that Defendant Kelley received $655,574 in incentives in 2016 for purportedly meeting certain performance targets, including $426,123 for meeting his Corporate Adjusted EPS target, $98,336 for meeting his "Corporate Operating Revenue" target, and $131,115 for meeting his "Individual Objectives" target. In support of Kelley purportedly meeting his performance targets, the 2017 Proxy Statement notes that Kelley achieved a rating of "Distinguished" on the following individual objectives for 2016:

- Directing and improving the effectiveness and efficiency of the Company's regulatory and government relations operations, including expanding government outreach programs, enhancing the Company's engagement with the Consumer Financial Protection Bureau and continuing legislative efforts (both in the U.S. and internationally).
- Continuing to improve business unit support and alignment.
- Continuing to refine and build out the Company's global security organization.

204. The 2017 Proxy Statement also noted that Defendant Ploder received $600,000 in incentives in 2016 for purportedly meeting certain performance targets, including $180,000 for meeting his Corporate Adjusted EPS target, $180,000 for meeting his "Workforce Solutions Operating Revenue" target, $120,000 for meeting

his "Workforce Solutions Operating Income" target, and $120,000 for meeting his "Individual Objectives" target. In support of Ploder purportedly meeting his performance targets, the 2017 Proxy Statement notes that Ploder achieved a rating of "Distinguished" on various individual objectives for 2016, including:

- Growing The Work Number instant employment verification database, expanding strategic partnerships and improving the Company's data analytic capability and use of trended data.

- Diversifying growth in verification services, including implementing targeted strategies and sales execution objectives to increase market share and deliver quality services and expanding channel partnerships and the enterprise selling model.

- Maximizing employer compliance with the Affordable Care Act.

- Leveraging talent strategy to source internal candidates to ensure Workforce Solutions has talent for future growth.

- Deploying strategies to provide solutions for client human resources compliance challenges, including developing a best in class compliance solution.

- Increasing our leadership position in unemployment claims management.

- Executing acquisition growth strategy, including identification of potential targets with desired strategic, financial and cultural characteristics.

205. The 2017 Proxy Statement stated the following regarding the Company's incentive compensation:

2016 Annual Cash Incentive Goals

Annual cash incentive awards are designed to reward the achievement of near-term business goals. In addition to financial metrics, annual incentive awards are based on an assessment of individual leadership qualities and contributions toward the achievement of business and strategic goals. When setting the range of performance goals for Corporate Adjusted EPS and Corporate Operating Revenue at the outset of the fiscal year, the Compensation Committee considered our financial results from the prior year and our annual operating budget for the coming year. The Committee also considered the history of attainment of goals in prior years, economic and industry conditions, industry sector performance and the views of our shareholders.

The 2016 corporate financial performance objectives for the NEOs with Company-wide responsibilities (Messrs. Smith, Gamble and Kelley and Ms. Rushing) were based on Corporate Adjusted EPS (used to measure profitability) and Corporate Operating Revenue (used to measure top line business growth). The financial objectives for Mr. Ploder, as business unit leader, were focused primarily on relevant business unit revenue and operating income performance (used to measure unit growth and profitability), as well as Corporate Adjusted EPS (to emphasize profitability of the Company as a whole).

Establishment of Corporate-Level Financial Goals

The Compensation Committee established corporate financial goals required to earn a cash incentive award for 2016 in a manner that is designed to, within reasonable limits, encourage achievement that exceeds target goals and penalize underachievement, while recognizing the need to encourage performance throughout the year. We set challenging, but realizable, goals, including those that are realizable only as a result of exceptional performance, for the Company and our executives in order to drive the achievement of our short- and long-term objectives.

206. Finally, in its "Governance Highlights," the 2017 Proxy Statement provided as follows regarding the Company's Enterprise Risk Management:

> We have a rigorous enterprise risk management program targeting controls over operational, financial, legal/regulatory compliance, reputational, technology, privacy, data security, strategic and other risks that could adversely affect our business. The program also includes crisis management and business continuity planning.

207. The 2017 Proxy Statement misrepresented and/or failed to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by harm they caused the Company; (vii) the Company had inadequate corporate financial-reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial

reporting; (x) the Company was recklessly relying on a single employee to address US-CERT warnings regarding critical data security systems; (xi) the Company had been warned by Deloitte in 2016 that Equifax was taking a careless approach to patching critical data security systems; (xii) Mandiant, in March or April 2017, had warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems; (xiii) the Company lacked a plan to quickly, effectively, and sufficiently respond to a major data breach; and (xiv) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times.

208. The false and/or misleading statements in the 2017 Proxy Statement were the essential link to the Director Defendants' reelection. Equifax shareholders voted for the 2017 Proxy Statement because of its false and/or misleading statements, and the losses to the Company resulted directly from the 2017 Proxy Statement vote—if the Director Defendants elected to the Board as a result of the 2017 Statement had not been elected to the Board, the Data Breach would likely not have occurred because basic data security measures would likely have been enacted.

VI. DEFENDANTS VIOLATED § 10(B) OF THE EXCHANGE ACT AND SEC RULE 10B-5, AND BREACHED THEIR FIDUCIARY DUTIES, BY KNOWINGLY OR RECKLESSLY ISSUING MATERIALLY FALSE AND MISLEADING STATEMENTS DURING THE RELEVANT PERIOD

A. The Director Defendants Caused Equifax to Conduct a Stock Repurchase Program Despite Their Knowledge That Critical Company Data Protection Mechanisms were Either Non-Existent or Defective

209. While the Company's shares were trading at artificially-inflated prices through misrepresentations and omissions of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton concerning the Company's financial and business prospects detailed in § VI.B, *infra*, the Director Defendants further propped up Equifax's stock price by causing the Company to repurchase millions of dollars' worth of its own common stock using Company (i.e., *shareholders*') funds.

210. In May 2010, the Company announced that its Board of Directors had

> authorized the repurchase of up to an additional $150 million of the company's common stock. Stock repurchases under this program may be made through open-market and privately negotiated transactions at times and in such amounts as management deems appropriate. The stock repurchase program does not have an expiration date and may be limited or terminated at any time without prior notice.

211. In September 2014, the Company announced that the Board approved an additional $400 million share repurchase authorization. This authorization was

in addition to the previous authorization, which had $141.7 million remaining as of June 30, 2014.

212. In May 2015, the Company announced that the Board authorized the repurchase of an additional 550 million dollars' worth of the Company's common stock, bringing the total remaining authorized share repurchase amount to $753 million as of April 30, 2015.

213. In connection with these authorizations, the Director Defendants caused Equifax to aggressively repurchase its shares, at prices that were artificially inflated based on Defendants' misrepresentations alleged herein. Indeed, in an apparent attempt to ostensibly improve its financial ratios and conceal the true facts concerning the Company's financial and business prospects, during 3Q17, the Company repurchased 535,901 of Equifax's common shares on the open market for $77.1 million, at an average price of $143.88 per share. This marked a dramatic departure from the Company's prior pattern of stock repurchases—the Company did not repurchase shares as part of its stock repurchase program in first or second quarter of 2017, or at any point in 2016.

214. In its 3Q17 10-Q, the Company stated, "[a]t September 30, 2017, the amount authorized for future share repurchases under the share repurchase program was $590.1 million." On the Company's November 10, 2017 conference call

discussing 3Q17 results with investors, Paulino do Rego Barros, Jr., who was appointed Interim CEO by the Company effective September 26, 2017, following Defendant Smith's departure, stated, "[o]n our last call, we had indicated that we would begin repurchasing shares in [3Q17]. We repurchased approximately $77 million in shares in 3Q17. However, given the cybersecurity incident, we have again suspended share repurchase activities. We do not intend to repurchase shares in 4Q17."

215. Despite the Director Defendants' knowledge of the true facts about the Company's business and financial prospects, these Defendants nevertheless authorized and executed the Company's purchases of its own stock at artificially-inflated prices. The Director Defendants' decisions were not the product of a valid business judgment because the Board knew during the repurchase period that the Company's stock was significantly inflated due to the false and misleading statements set forth in this Complaint.

216. Because the price of the Company's shares was artificially inflated due to the concealment and misrepresentations by certain Defendants, the Company materially overpaid for its own stock. All told, between July 1, 2017 and August 31, 2017, Equifax repurchased 535,901 of its own shares, at inflated average quarterly prices, ranging from $145.29 and $143.60 per share (an average price of $144.445),

for a total of over $77 million. By September 15, 2017, the value of this stock had declined to approximately $49.8 million—a 35.4% decline, constituting $27.28 million in shareholders' funds that had simply evaporated.

217. The repurchases falsely signaled to the Company's shareholders and the public that the purchase of Equifax stock at those prices was the best use of the Company's cash and the purchases of the stock at the market price prevailing at that time represented a good value for the Company. In truth, the Company's expenditures on its own stock were so recklessly improvident as to constitute corporate waste. The repurchases were not designed to serve a legitimate corporate interest. Rather, they were designed to help conceal the true facts concerning Defendants' misrepresentations and omissions through an inflated stock price.

B. In Connection with the Company's 3Q17 Share Repurchases, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton Issued False or Misleading Statements Regarding Data Security and Related Topics

218. On February 22, 2017, after the market closed, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton caused the Company to file the 2016 10-K, reporting the Company's financial and operating results for 4Q16 and fiscal year 2016 ("FY16"). For 4Q16, the Company reported unaudited revenue of $801.1 million (or $1.01 per

diluted share), an increase in revenue of 20% compared to the same quarter in the prior year. For FY16, the Company reported revenue of $3.1 billion (or $4.04 per diluted share), an increase in revenue of 18% compared to the previous year. The 2016 10-K represented that the Company's disclosure controls and procedures were effective as of December 31, 2016. The Company's 2016 10-K also provided as follows:

> ***Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.***
>
> In the ordinary course of business, we rely upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including business-to-business and business-to-consumer electronic commerce and internal accounting and financial reporting systems. Additionally, ***we collect and store sensitive data, including*** intellectual property, proprietary business information and ***personally identifiable information of our customers,*** employees, consumers and suppliers, ***in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.***
>
> Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, ***our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to*** damage, disruptions, shutdowns, or ***breaches of confidential information due to criminal conduct, denial***

> ***of service or other advanced persistent attacks by hackers,*** employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. ***Unauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.***
>
> ***We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact.*** Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. ***Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations.*** Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Also, our third-party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

219. The 2016 10-K also discussed Equifax's business strategy, stating in pertinent part:

> **OUR BUSINESS STRATEGY**
>
> Our strategic objective is to be the global leader in information solutions that creates unparalleled insights to solve customer

challenges. ***Data is at the core of our value proposition.*** Leveraging our extensive resources, we deliver differentiated decisions through a broad and diverse set of data assets, sophisticated analytics and proprietary decisioning technology. Our long-term corporate growth strategy is driven by the following imperatives:

- Deliver consistently strong profitable growth and shareholder returns. We seek to meet or exceed our financial commitments on revenue growth and margins through disciplined execution of our strategic initiatives and by positioning ourselves as a premier provider of high value information solutions.

- Develop unparalleled analytical insights leveraging Equifax unique data. We continue to invest in and acquire unique sources of credit and non-credit information to enhance the variety and quality of our services while increasing clients' confidence in information-based business decisions. Areas of focus for investment in new sources of data include, among others, positive payment data, fraud and personal identification data, real estate data and new commercial business data. We also have developed unique capabilities to integrate customer and third-party data into our solution offerings to further enhance the decisioning solutions we develop for our customers.

  We continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of the services we offer and further differentiate our products from those offered by our competitors. In addition to custom products for large clients, we develop software as a service based, decisioning and data access technology platforms that are more cost effective for clients of all sizes. We also develop predictive scores and analytics, some of which leverage multiple data assets, to help clients acquire new customers and manage their existing customer relationships. We develop a broad array of industry, risk management, cross-sell and account acquisition models to enhance the precision of our clients' decisioning activities. We also develop custom and generic solutions that enable customers

> to more effectively manage their debt collection and recovery portfolios.
>
> * * *
>
> - ***Serve as a trusted steward and advocate for our customers and consumers.*** This includes continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, ***while simultaneously delivering security for*** [the Company's] ***services.***

220. The 2016 10-K was signed by Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, and contained signed certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX") by Defendant Smith (in his capacity as Equifax's CEO and Chairman) and Defendant Gamble (in his capacity as Equifax's CFO), which certified as follows:

> 1. I have reviewed this annual report on Form 10-K of Equifax Inc.;
>
> 2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
>
> 3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15(d)-15(f)) for the registrant and have:

   a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over

> financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):
>
> a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and
>
> b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

221. In addition, the representation in the 2016 10-K that the Company was purportedly "not aware of any material breach of [its] data, properties, networks or systems" was demonstrably false and misleading. Indeed, Equifax had experienced myriad, substantial data breaches in 2016, and years prior, of which the directors would have been aware at the time of the time of the filing of the 2016 10-K. *See* § IV.C, *supra*.

222. On April 26, 2017, the Individual Defendants caused Equifax to file a current report on Form 8-K with the SEC, attaching, as an exhibit, a press release that was issued that same day, announcing, among other things, the Company's financial and operating results for the first quarter of 2017 ("1Q17") and the six months ended March 31, 2017. For 1Q17, the Company reported unaudited revenue

of $832.2 million, or $1.26 per diluted share, an increase in revenue of 14% compared to the same quarter in the prior year.

223. On April 27, 2017, the Individual Defendants caused Equifax to file its quarterly report on Form 10-Q with the SEC (the "1Q17 10-Q"), reporting the Company's financial and operating results for 1Q17. The 1Q17 10-Q disclosed an increase in the Company's capital expenditures which, among other purposes, purportedly served to improve "system reliability, security and disaster recovery enhancements." To that end, the 1Q17 10-Q stated, in relevant part:

Investing Activities

Capital Expenditures

Net cash used in:	Three Months Ended March 31, 2017	2016	Change 2017 vs. 2016
	(In millions)		
Capital expenditures*	$ (50.3)	$ (40.2)	$ (10.1)

*Amounts above include cash outflows for capital expenditures.

Our capital expenditures are used for developing, enhancing and deploying new and existing software in support of our expanding product set, replacing or adding facilities and equipment, updating systems for regulatory compliance, the licensing of software applications and investing in system reliability, security and disaster recovery enhancements. Capital expenditures in the first three months of 2017 increased by $10.1 million from the same period in 2016 as we paid amounts that were accrued as of December 31, 2016.

224. The 1Q17 10-Q was signed by Defendants Smith and Gamble, and contained certifications pursuant to SOX signed by Defendant Smith (in his capacity as CEO and Chairman of the Board) and Gamble (in his capacity as CFO) that were substantially similar to those identified above in ¶220.

225. On June 1, 2017, the Individual Defendants caused the Company to hold an investor presentation (the "June 1, 2017 Presentation"), during which the reliability of Company's data security was touted in the following slide:

226. During a Stephens Investor Conference held June 7, 2017, Defendant Gamble spoke on behalf of the Company regarding, *inter alia*, its businesses and products, stating that Equifax's Workforce Solutions Segment, which had grown substantially over the previous five years, was driven in part by the Company's info exchange service, which purportedly "***provides a secure verification network*** where the contributors, as an employer contributes information into our exchange, ***we make sure that the people accessing that information have a right to see it***."

227. On July 26, 2017, the Individual Defendants caused Equifax to file a current report on Form 8-K with the SEC, attaching as an exhibit a press release that was issued that same day (the "July 26, 2017 Press Release"), announcing, among other things, the Company's financial and operating results for the second quarter of 2017 ("2Q17") and the six months ended June 30, 2017. For 2Q17, the Company reported unaudited revenue of $856.7 million (or $1.36 per diluted share), an increase in revenue of 6% compared to the same quarter in the prior year. Throughout the press release, the Company disclosed strong revenue growth driven by identity and fraud solutions. To that end, the July 26, 2017 Press Release stated, in pertinent part:

Strong execution, revenue growth and margin expansion drive double-digit EPS growth

- Revenue of $856.7 million was up 6 percent (7 percent in local currency) compared to the second quarter of 2016.
- Diluted EPS of $1.36 was up 26 percent compared to the second quarter of 2016.
- Adjusted EPS of $1.60 was up 12 percent compared to the second quarter of 2016.
- Net income attributable to Equifax of $165.4 million was up 26 percent compared to the second quarter of 2016.
- Adjusted EBITDA margin was 39.1 percent compared to 36.6 percent in the second quarter of 2016.

ATLANTA, July 26, 2017 -- Equifax Inc. (NYSE: EFX) today announced financial results for the quarter ended June 30, 2017.

"***Second quarter performance reflects outstanding execution by the team*** and the strength of our unique portfolio of businesses," said Richard F. Smith, Chairman and Chief Executive Officer at Equifax. "The team continues to make significant progress on new product innovation and our enterprise growth initiatives, both in the U.S. and around the world. We remain confident in our outlook for 2017 and are optimistic about the opportunities in front of us as we look ahead to 2018."

Financial Results Summary

The company reported revenue of $856.7 million in the second quarter of 2017, a 6 percent increase compared to the second quarter of 2016 on a reported basis and up 7 percent on a local currency basis.

Second quarter diluted EPS attributable to Equifax was $1.36, up 26 percent compared to the second quarter of 2016. Adjusted EPS attributable to Equifax was $1.60, up 12 percent compared to the second quarter of 2016. This financial measure for 2017 excludes the income

tax effects of stock awards recognized upon vesting or settlement and for 2016 excludes Veda acquisition related amounts. The financial measure for both 2017 and 2016 excludes acquisition-related amortization expense, net of associated tax impacts. These items are described more fully in the attached Q&A.

Net income attributable to Equifax of $165.4 million was up 26 percent compared to the second quarter of 2016. Adjusted EBITDA margin was 39.1 percent, compared to 36.6 percent in the second quarter of 2016. These financial measures for 2017 and 2016 have been adjusted for certain items, which affect the comparability of the underlying operational performance and are described more fully in the attached Q&A.

USIS delivered strong revenue growth driven by mortgage, marketing and analytic services, and identity and fraud solutions.

- Total revenue was $331.9 million in the second quarter of 2017 compared to $307.9 million in the second quarter of 2016, an increase of 8 percent. Operating margin for USIS was 45.1 percent in the second quarter of 2017 compared to 43.5 percent in the second quarter of 2016. Adjusted EBITDA margin for USIS was 51.5 percent in the second quarter of 2017 compared to 50.4 percent in the second quarter of 2016.

- Online Information Solutions revenue was $232.6 million, up 6 percent compared to the second quarter of 2016.

- Mortgage Solutions revenue was $38.6 million, up 10 percent compared to the second quarter of 2016.

- Financial Marketing Services revenue was $60.7 million, up 15 percent compared to the second quarter of 2016.

* * *

Third Quarter 2017 and Full Year 2017 Outlook

We are off to a strong start through the first half of 2017. For the third quarter, at current exchange rates, we expect revenue to be between

> $853 and $861 million, reflecting growth of 6-7%, with limited foreign exchange impact. Adjusted EPS is expected to be between $1.50 and $1.54 which is up 4% to 7%, also with limited foreign exchange impact.
>
> We expect full year 2017 revenue to be between $3.395 and $3.425 billion, reflecting constant currency growth of approximately 9%. Adjusted EPS for the year is expected to be between $6.02 and $6.10, which is up approximately 10%.

228. On July 27, 2017, the Individual Defendants caused the Company to file its quarterly report on Form 10-Q with the SEC (the "2Q17 10-Q"), reporting the Company's financial and operating results for 2Q17. The 2Q17 10-Q disclosed an increase in the Company's capital expenditures which, among other purposes, purportedly served to improve "system reliability, security and disaster recovery enhancements." To that end, the 2Q17 10-Q stated, in relevant part:

> **Investing Activities**
>
> **Capital Expenditures**

Net cash used in:	Six Months Ended June 30, 2017	2016	Change 2017 vs. 2016
	(In millions)		
Capital expenditures*	$(99.9)	$(82.8)	$ (17.1)

> *Amounts above are total cash outflows for capital expenditures.
>
> Our capital expenditures are used for developing, enhancing and deploying new and existing software in support of our expanding product set, replacing or adding facilities and equipment, updating systems for regulatory compliance, the licensing of software

> applications and investing in system reliability, security and disaster recovery enhancements. Capital expenditures in the first six months of 2017 increased by $17.1 million from the same period in 2016 as we paid amounts that were accrued as of December 31, 2016.

229. The 2Q17 10-Q was signed by Defendants Smith and Gamble, and contained certifications pursuant to SOX signed by Defendant Smith (in his capacity as CEO and Chairman of the Board) and Gamble (in his capacity as CFO) that were substantially similar to those identified above in ¶220.

230. On August 16, 2017, the Individual Defendants caused the Company to hold another investor presentation (the "August 16, 2017 Presentation"), during which the reliability of Company's data security was touted in a slide identical to the one presented in the June 1, 2017 Presentation (*see* ¶225).

231. During the August 17 Terry College Speech, Smith frequently discussed security issues relating to the Company's large database. "When you have the size database we have, it's very attractive for others to try to get into our database," admitted Smith, "[s]o it is a huge priority for us." During the speech, Smith was asked specifically about data fraud and security. "Fraud is a huge opportunity for us. It is a massive, growing business for us," he said.

232. The statements referenced above in ¶¶218–231 were materially false and misleading because the Individual Defendants made false and/or misleading statements, as well as failed to disclose material adverse facts regarding the

Company's business practices, operations, financials, compliance policies and practices, and internal controls. Specifically, the Individual Defendants made, or caused the Company to make, false and/or misleading statements, and/or failed to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by harm they caused the Company; (vii) the Company had inadequate corporate financial-reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial reporting; (x) the Company was recklessly relying on a single employee to address

US-CERT warnings regarding critical data security systems; (xi) the Company had been warned by Deloitte in 2016 that Equifax was taking a careless approach to patching critical data security systems; (xii) Mandiant, in March or April 2017, had warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems; (xiii) the Company lacked a plan to quickly, effectively, and sufficiently respond to a major data breach; and (xiv) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times. As a result of this fraud, the Individual Defendants were able to artificially inflate the Company's financials, and its stock price, during the Relevant Period.

C. The Insider Selling Defendants Unlawfully Profited at Equifax's Expense by Selling Back Shares to the Company at Artificially-Inflated Prices

233. Not all shareholders were harmed by the Individual Defendants' actions. Indeed, between February 22, 2017 and August 2, 2017, while in possession of material, adverse, and non-public information, the Insider Selling Defendants (including Defendants Smith, Gamble, Kelley, Ploder, and Loughran) unloaded significant amounts of their personal holdings of Equifax stock at artificially-inflated prices. Specifically, the Insider Selling Defendants took advantage of the

artificially-inflated prices to sell their personally-held Equifax shares for substantial proceeds. As detailed below, these Insider Selling Defendants sold ***nearly $15 million*** in personally-held Equifax common stock between February 22, 2017 and August 2, 2017.

234. Smith was Equifax's long-time CEO and Chairman of the Board, including at the time of the misconduct alleged herein, from December 15, 2005 until his "retirement" on September 26, 2017. During the Relevant Period, Smith was aware of material, adverse, and non-public information, including the fact that the Company was being operated by the Individual Defendants in evident violation of the law, as well as the inaccuracy of the Company's statements in press releases and public filings, and those made by other senior executives at Equifax. While in possession of this information, Smith sold at least 73,346 personally-held shares on February 28, 2017, at the artificially-inflated price of $131.037 per share, for proceeds of $9,742,076.80. Smith's sales were timed to maximize profits from the Company's then artificially-inflated stock price.

235. Defendant Gamble is the current CFO and Corporate Vice President of the Company, which are roles he has held since May 2014. During the Relevant Period, Gamble was aware of material, adverse, and non-public information, including the fact that the Company was being operated by the Individual

Defendants in evident violation of the law, as well as the inaccuracy of the Company's statements in press releases and public filings, and those made by other senior executives at Equifax. While in possession of this information, Gamble sold at least 20,500 personally-held shares of Equifax stock (i.e., nearly 33% of his total holdings), at artificially-inflated prices, for total proceeds of $2,856,506, including 14,000 shares on May 23, 2017, at $136.4380 per share, for proceeds of $1,910,132, and 6,500 shares on August 1, 2017, at $145.5960 per share for proceeds of $946,374. Gamble's sales were suspiciously timed to maximize profits from the Company's then artificially-inflated stock price. Indeed, despite Gamble serving as the Company's CFO and Corporate Vice President since May 2014, Gamble's May 23, 2017 sale was the first time Gamble had engaged in insider trading at the Company.

236. Defendant Kelley is the current Chief Legal Officer, Corporate Vice President, and Corporate Secretary, which are roles he has held since January 2013. During the Relevant Period, Kelley was aware of material, adverse, and non-public information, including the fact that the Company was being operated by the Individual Defendants in evident violation of the law, as well as the inaccuracy of the Company's statements in press releases and public filings, and those made by other senior executives at Equifax. While in possession of this information, on

February 28, 2017, Kelley sold at least 8,500 personally-held shares of Equifax stock (i.e., nearly 42% of his total holdings), at artificially-inflated prices ($130.8471 per share), for total proceeds of $1,112,845.27. Kelley's sales were timed to maximize profits from the Company's then artificially-inflated stock price. Despite serving as Chief Legal Officer, Corporate Vice President, and Corporate Secretary since January 1, 2013, Kelley's February 28, 2017 sales were (i) only the third time Kelley had ever conducted insider sales at the Company, and (ii) his first insider sales at the Company since February 18, 2016.

237. Defendant Ploder is the current President of Workforce Solutions for the Company, a role he has held since November 2014. During the Relevant Period, Ploder was aware of material, adverse, and non-public information, including the fact that the Company was being operated by the Individual Defendants in evident violation of the law, as well as the inaccuracy of the Company's statements in press releases and public filings, and those made by other senior executives at Equifax. While in possession of this information, Ploder sold at least 1,719 personally-held shares of Equifax stock on August 1, 2017, at the artificially-inflated price of $145.70 per share, for proceeds of $250,458.30. Ploder's sales were timed to maximize profits from the Company's then artificially-inflated stock price.

238. Defendant Loughran is the current President of U.S. Information Solutions for the Company, and has served in various executive roles for the Company since March 2006. During the Relevant Period, Loughran was aware of material, adverse, and non-public information, including the fact that the Company was being operated by the Individual Defendants in evident violation of the law, as well as the inaccuracy of the Company's statements in press releases, public filings, and in statements made by other senior executives at Equifax. While in possession of this information, Loughran sold at least 4,000 personally-held shares of Equifax stock on August 1, 2017, at the artificially-inflated price of $146.0247 per share, for total proceeds of approximately $584,098.80. Loughran's sales were timed to maximize profits from the Company's then-artificially inflated stock price.

239. The foregoing insider sales, which resulted in total proceeds of ***nearly $15 million***, are summarized in the following chart:

Insider	**Date**	**Shares**	**Price**	**Proceeds**
Smith	February 28, 2017	74,346	$131.0370	$9,742,076.80
	TOTAL	**74,346**		**$9,742,076.80**
Gamble	August 1, 2017	6,500	$145.5960	$946,374.00
	May 23, 2017	14,000	$136.4380	$1,910,132.00
	TOTAL	**20,500**		**$2,856,506.00**
Kelley	February 28, 2017	8,500	$130.8471	$1,112,200.35
	TOTAL	**8,500**		**$1,112,200.35**

Ploder	August 2, 2017	1,719	$145.7000	$250,458.30
	TOTAL	**1,719**		**$250,458.30**
Loughran	August 1, 2017	4,000	$146.0247	$584,098.80
	TOTAL	**4,000**		**$584,098.80**
TOTAL INSIDER SALES		**109,065**		**$14,545,340.25**

240. These insider sales were all executed under highly suspicious circumstances and occurred while the Company's stock price was artificially inflated due to the unlawful conduct and the misrepresentations and omissions alleged herein, specifically including the Individual Defendants' awareness that the Company was being operated in a manner that made it highly susceptible to committing the precise unlawful conduct alleged herein, and the Individual Defendants' failure to prevent the same by ensuring that the Company implemented and maintained reasonably adequate data security measures to safeguard and protect data maintained by the Company.

241. The 12,219 shares sold by Defendants Gamble, Loughran, and Ploder, for total proceeds of $1,780,931.10, in a 48-hour span from August 1, 2017 to August 2, 2017, are even more suspicious. Given the Company's claim that it purportedly first learned of the Data Breach on July 29, 2017, these sales were made ***within mere days*** of such discovery, but ***more than a month*** before the Data Breach was finally disclosed to the public. These sales were timed immaculately, as the

precipitous decline in the Company's stock price following the Company's disclosure of the Data Breach on September 7, 2017, would result in those same shares being worth much less).[50]

242. Because of their roles as directors and/or officers of Equifax during the Relevant Period, the Insider Selling Defendants either knew, consciously disregarded, were reckless and grossly negligent in not knowing, or should have known material, adverse, and non-public information about the Company's business practices, operations, financials, compliance policies and practices, and internal controls, including, *inter alia*, that the unlawful conduct and the false and misleading statements alleged herein caused the price of the Company's stock to trade at artificially-inflated prices at the same time the Insider Selling Defendants were disposing of millions of dollars' worth of Company stock. These Insider Selling Defendants had a duty not to sell shares while in possession of material, adverse, non-public information concerning Equifax's business practices, operations, financials, compliance policies and practices, and internal controls, but they egregiously violated this duty.

[50] On September 8, 2017, immediately following disclosure of the Data Breach, the Company's stock price tumbled $19.49 per share (or approximately 13.7%), on unusually high trading volume, to close at $123.23 per share.

243. Incredibly, on November 3, 2017, the Company published a press release announcing the findings of a Special Committee of the Board relating to the "securities trading matter." According to the press release, the Company formed the Special Committee in September 2017 and examined whether the trades of Gamble, Loughran, Ploder, and Douglas G. Brandberg ("Brandberg") (Senior Vice President, Investor Relations), comported with the Company's Insider Trading Policy, whether the executives had any information about the security incident when they made their trades, and whether preclearance was appropriately obtained.

244. The Special Committee's report (the "Special Committee Report"), which was attached to the November 3, 2017 press release, concluded that "none of the four executives had knowledge of the incident when their trades were made, that preclearance for the four trades was appropriately obtained, that each of the four trades at issue comported with Company policy, and that none of the four executives engaged in insider trading." As part of the review process, the Special Committee purportedly conducted dozens of interviews, and reviewed more than 55,000 documents, including emails, text messages, phone logs, and other records.

245. The Special Committee Report found each executive sought and received clearance from the appropriate Legal Department personnel prior to trading. Based on its review, the Committee concluded that neither Equifax's Chief

Legal Officer (Defendant Kelley) nor his "designated preclearance officer" had reason to believe that Messrs. Gamble, Loughran, Ploder, or Brandberg had knowledge of the security incident's existence as of the date of their preclearance requests or the date of their trades. Accordingly, the Special Committee concluded that the preclearance authorization obtained by Messrs. Gamble, Loughran, Ploder, and Brandberg was within the authority permitted under the policy obtained preclearance for the trades.

246. The Special Committee Report offers no explanation, however, as to why Equifax's Legal Department and Equifax's Chief Legal Officer, Kelley, approved some of the stock sales on the same day that he called to alert the FBI of the Data Breach, or why the Company waited until August 15, 2017, to impose a trading blackout on all Company personnel identified as aware of the breach as of that date.

D. In Repurchasing Stock, Equifax Relied on the False and Misleading Statements of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton

247. In repurchasing shares in connection with the stock repurchase program, Equifax relied on the false or misleading statements of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, either directly or through the "fraud on the market" doctrine.

248. At all relevant times, the market for Equifax common stock was an efficient market, for many reasons. Equifax stock met the requirements for listing, and was listed and actively traded on the NYSE, a highly efficient and automated market. According to the Company's 3Q17 10-Q, filed November 9, 2017, the Company had more than 120 million shares outstanding as of September 30, 2017. Hundreds of thousands of shares of Equifax stock are traded on a daily basis, demonstrating a very active and broad market for Equifax stock, and permitting a very strong presumption of an efficient market. Equifax claims to be qualified to file a less comprehensive Form S-3 registration statement with the SEC that is reserved, by definition, to well-established and largely capitalized issuers for whom less scrutiny is required. As a regulated issuer, Equifax filed periodic public reports with the SEC and the NYSE. Equifax regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services. Finally, Equifax was followed by several securities analysts employed by major brokerage firms who wrote reports which were distributed to the sales force and certain customers of their respective

brokerage firms. Each of these reports was publicly available and entered the public marketplace.

249. As a result of the foregoing, the market for Equifax common stock promptly digested current information regarding Equifax from all publicly available sources and reflected such information in the price of Equifax common stock. Under these circumstances, all purchasers of Equifax common stock during the Relevant Period suffered similar injury through their purchase of Equifax common stock at artificially-inflated prices, and a presumption of reliance thus applies.

250. Had Equifax known of the material adverse information not disclosed by Defendants, or had Equifax been aware of the truth behind the material misstatements of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton Company would not have repurchased Equifax stock at artificially-inflated prices.

E. Neither the Statutory "Safe Harbor" Nor the "Bespeaks Caution" Doctrine Applies to the Misrepresentations of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton

251. Neither the safe-harbor provision of the Private Securities Litigation Reform Act of 1995 (the "PSLRA") nor the judicially created "bespeaks caution" doctrine applicable to forward-looking statements under certain circumstances applies to any of the false or misleading statements pleaded in this Complaint. None

of the subject statements constituted a forward-looking statement; rather, they were historical statements or statements of purportedly current facts and conditions at the time the statements were made, including statements about Equifax's data security controls and systems, its present financial condition, and its internal controls, among other things.

252. Alternatively, to the extent any of the false or misleading statements pleaded in this Complaint could be construed as forward-looking statements, they were not accompanied by any meaningful, cautionary language identifying important facts that could cause actual results to differ materially from those in the purportedly forward-looking statements. Further, to the extent the PSLRA's safe harbor would otherwise apply to any forward-looking statements pleaded in this Complaint, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton are liable for those false or misleading statements because, at the time each of those statements was made, the speaker(s) knew the statement was false or misleading, or the statement was authorized or approved by an executive of Equifax or an Individual Defendant who knew the statement was materially false or misleading when made.

F. The Group Pleading Doctrine Applies to the Misstatements and Omissions of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton

253. All of Plaintiffs' claims against the Individual Defendants essentially allege that they are liable because of information they received and decisions they made collectively. There is nothing to be gained by addressing each Individual Defendant individually because they are all similarly situated.

254. The Individual Defendants participated in the drafting, preparation, or approval of the various shareholder and investor reports, and other communications concerning Equifax identified in this Complaint, and were aware of, or recklessly disregarded, the misstatements contained in those reports and other communications, as well as the omissions from them, and were aware of their materially false and misleading nature. Each Individual Defendant, by virtue of his or her position(s) at Equifax, had access to adverse, undisclosed information about the Company's business prospects, financial condition, and performance as alleged in this Complaint, and knew or recklessly disregarded that those adverse facts rendered the subject statements materially false or misleading when made.

255. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, because of their positions of control and authority as officers or directors of Equifax, were able to, and did, control

the content of the various SEC filings, press releases, and other public statements pertaining to the Company during the Relevant Period.

256. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton were provided with copies of the documents alleged in this Complaint to be false or misleading prior to or shortly after their issuance, or had the ability or opportunity to prevent their issuance or to cause them to be corrected. Accordingly, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton are responsible for the accuracy of the public reports, releases, and other statements detailed in this Complaint, and are therefore primarily liable for the misrepresentations in them or misleading omissions from them.

G. The Misstatements and Omissions of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton Caused Damages to Equifax.

257. In response to Equifax's disclosures regarding the Data Breach, the Company's stock price tumbled $19.49 per share (or approximately 13.7%), on unusually high trading volume, to close at $123.23 per share on September 8, 2017, resulting in a loss of approximately $2.34 billion in market capitalization. And in the days that followed, the stock continued declining at a catastrophic rate, reaching a low of $92.98 at the close of trade on September 15, 2017 (eight days after the

Data Breach was disclosed), representing a decline of $49.74 (or approximately 34.9%) per share, and a loss of approximately $6 billion in market capitalization, compared to the share price at close of trade on September 7, 2017 (the day before disclosure of the Data Breach).

258. The decline in Equifax's share price was a direct result of the nature and extent of Defendants Smith's, Gamble's, Daleo's, Driver's, Feidler's, Hough's, Humann's, Marcus's, Marshall's, McKinley's, Stock's, and Templeton's fraud finally being revealed to the market. The timing and magnitude of the decline in the Company's share price negates any inference that the losses suffered by Equifax were caused by changed market conditions, macroeconomic or industry factors, or Company-specific facts unrelated to the fraudulent conduct of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton.

VII. DAMAGES TO THE COMPANY AND ITS SHAREHOLDERS

259. As a result of the Individual Defendants' wrongful conduct, the business of Equifax was operated in evident violation of, *inter alia*, myriad federal, state, and municipal laws, rules, and regulations, and the Company disseminated false and misleading statements and omitted material information to make such statements not false and misleading when made. The improper statements have

devastated Equifax's credibility. Equifax has been, and will continue to be, severely damaged and injured by the Individual Defendants' misconduct.

260. As a direct and proximate result of the Individual Defendants' actions as alleged above, Equifax's market capitalization has been substantially damaged, having lost billions of dollars in value as a result of the conduct described herein.

261. Further, as a direct and proximate result of the Individual Defendants' misconduct, Equifax has expended at least $87.5 million in connection therewith as of the time of the filing of the Complaint, and will continue to expend significant sums of money. Such expenditures include, but are not limited to:

(a) costs incurred in investigating and defending Equifax and certain officers and directors in the Securities Class Actions, the Consumer Class Actions, and the Consumer Protection Actions, plus potentially millions of dollars in settlement or to satisfy adverse judgments;

(b) costs incurred by the Company in connection with the countless high-profile investigations and probes launched into Equifax's unlawful business operations and public disclosures in connection with the Data Breach, including but not limited to, by the SEC, FBI, DOJ, FTC, CFPB, multiple Congressional committees, State Attorney Generals and foreign governments;

(c) costs incurred from the misappropriation of Company information by the Insider-Selling Defendants for the purpose of selling Equifax common stock at artificially-inflated prices;

(d) costs incurred from compensation and benefits paid to the Individual Defendants, which compensation was based at least in part on Equifax's artificially-inflated stock price;

(e) costs associated with the repurchase of Company shares at prices that were artificially inflated, including nearly $77 million spent to reacquire stock at prices artificially inflated by the misstatements and/or omissions of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton; and

(f) costs incurred from the loss of the Company's customers' and regulators' confidence in Equifax's products.

262. Moreover, these actions have irreparably damaged Equifax's corporate image and goodwill. For at least the foreseeable future, Equifax will suffer from what is known as the "liar's discount," a term applied to the stocks of companies who have been implicated in illegal behavior and have misled the investing public, such that Equifax's ability to raise equity capital or debt on favorable terms in the future is now impaired.

263. As a result of the Individual Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Equifax has suffered significant losses and damages. The fallout resulting from the Data Breach has been severe, and has caused the Company to suffer significant damages and harm far above and beyond the loss of billions of dollars in market capitalization resulting from the precipitous decline in the Company's stock price, as well as its corporate goodwill.

264. On Friday, September 8, 2017, an article[51] discussing various analysts' perspectives on the ultimate costs of the Data Breach was published by CNBC, stating, *inter alia*, as follows:

> Analysts are worried Equifax's data breach crisis may cost the company hundreds of millions of dollars and hurt its reputation for years to come.
>
> Equifax, which supplies credit information and other information services, revealed on Thursday that it suffered a data breach that could potentially affect 143 million consumers. The company said 209,000 credit card numbers were obtained, in addition to "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers."
>
> Shares of Equifax plummeted 13.2 percent Friday in the wake of the announcement. If the stock closes at this level, it would be the largest single-day drop since August 20, 1999.

[51] Tae Kim, *Equifax shares plunge the most in 18 years as Street says breach will cost company hundreds of millions*, CNBC, https://www.cnbc.com/2017/09/08/equifax-plunges-as-breach-will-cost-company-hundreds-of-millions.html (last visited Jan. 17, 2018).

> Stifel compared the incident with previous cybersecurity breaches at prominent retailers.
>
> The "significant data breach is likely to cost the company materially, and costs could drag on for a number of years," analyst Shlomo Rosenbaum wrote in a note to clients Friday. "We aren't changing estimates right now because of lack of clarity, though clearly ours and consensus estimates are too high in the near term."
>
> In similar fashion, SunTrust also focused on the negative impact to the company's credibility with consumers.
>
> "This is clearly a material event, in our opinion. The breach compromises Equifax's reputation as a trusted steward of consumer data, and will create a near-term business disruption, per the company's public comments," analyst Andrew Jeffrey wrote in a note to clients Thursday.
>
> Equifax shares had outperformed the market this year before the news. Its stock rallied 21 percent year to date through Thursday versus the S&P 500's 10 percent return.
>
> To assess the potential costs for Equifax, Stifel's Rosenbaum cited the large credit card breaches at Target in 2013 and Home Depot in 2014, when hackers got access information on tens of millions of customers.
>
> "Based on large scale breaches at Target and Home Depot, we believe $300M-$325M in gross costs for the breach would not be unreasonable," he wrote.
>
> Cowen analyst George Mihalos added "based on prior cyber security incidents, we would be unsurprised to see a total cost exceeding $200 million" in a report Thursday.

265. Additionally, shortly after the Data Breach was finally revealed to the public, hundreds of class action lawsuits were filed nationwide against the Company—and in some of the lawsuits, against certain of the Company's executives

and directors—in the form of the Securities Class Actions, the Consumer Class Actions, and the Consumer Protection Actions. In addition, countless high-profile investigations and probes have been launched into Equifax in connection with the Data Breach, including by the SEC, FBI, U.S. Department of Justice, FTC, CFPB, several committees of the U.S. Senate and House of Representatives, Attorney Generals of all 50 states, along with Washington D.C., and Puerto Rico, and the British and Canadian governments. On December 6, 2017, the Panel transferred 76 civil actions to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407, creating the Consumer MDL.

266. Numerous regulatory actions are proceeding against the Company. On November 20, 2017, Trey Gowdy, chairman of the House Government Reform Committee, and Lamar Smith, chairman of the House Science, Space, and Technology Committee, sent a letter to the Company's newly appointed interim CEO, Paulino do Reggo Barros, Jr., demanding certain information by December 6, 2017. The letter demanded the Office of the CIO of Equifax turn over "documents sufficient" to identify the names and titles of all individuals working in the CIO's office between March and the present date. The chairmen also demanded "all organizational charts" or documents sufficient to reflect the roles and responsibilities of all employees in the office of the CIO during the same period. '

267. The letter also demanded that the Company's CIO office provide (i) any communications it has between any federal agency and Equifax and any Homeland Security Department "reports and recommendations" to Equifax concerning the Data Breach; (ii) any documents identifying any prior data breaches on its network from January 2014 to the time it discovered the Data Breach; (iii) the names and titles of staffers who worked in the Office of the CSO; (iv) documents containing the roles and responsibilities of CSO employees; (v) any communications between former CSO Susan Mauldin relating to Apache Struts 2—the software that hackers exploited in the Data Breach and the application that Equifax uses in its online disputes portal—that occurred between March and September 2017; (vi) the name and title of the individual who failed to forward a March 8, 2017 alert from U.S.-CERT to Equifax and many other companies about the need to patch a vulnerability in Apache Struts 2; (vii) the names and titles of any individuals on the distribution list for cyber-threat and other critical email alerts, "specifically those individuals" who received the March 9, 2017 internal distribution of U.S.-CERT's alert; and (viii) names and titles of individuals who formed the Company's incident response team, including contractors.

268. Equifax does not have sufficient insurance coverage to protect the Company from losses stemming from the Data Breach. According to a Bloomberg

article[52] citing "people familiar with the [insurance] coverage," Equifax holds an insurance policy covering between $100 million and $150 million of costs associated with the Data Breach. The Company will likely have to pay multiple times that amount in related penalties, settlements, and/or judgments.

269. On the Company's November 10, 2017 conference call discussing 3Q17 results with investors, Gamble stated the Company had already incurred a one-time charge in 3Q17 of $87.5 million, stating,

> In 3Q[17], we incurred a onetime charge related to the cybersecurity incident of $87.5 million. These costs were included in our non-GAAP adjustments. $27.3 million of costs for the -- for third-party services provided principally in the investigation of the cybersecurity incident. These costs were generally for legal, cyber forensic investigations and other professional services.

270. Indeed, on November 29, 2017, the action captioned *Katiushka Rebeca Acosta-Smith, et al. v. Equifax Inc.*, filed on October 23, 2017, in the Superior Court for Orange County, California, was removed to the U.S. District Court for the Central District of California. In its Notice of Removal, the Company identified a number of cases in which courts have awarded verdicts and judgments for hundreds of thousands of dollars for claims arising from the improper handling of PII:

[52] Sonali Basak and Jennifer Surane, *Equifax's Insurance Is Likely Inadequate for Breach*, Bloomberg https://www.bloomberg.com/news/articles/2017-09-09/equifax-s-insurance-said-likely-to-be-inadequate-against-breach (last visited Sept. 9, 2017).

The Ninth Circuit recently upheld a jury verdict of $150,000 in noneconomic damages to a victim of identity theft who claimed that the defendant insufficiently handled his claim. *Sungtae Kim v. BMW Financial Services NA LLC*, No. 15-56801, mem. op. (9th Cir. July 31, 2017) (attached as Exhibit G). A California District Court awarded $315,000 in emotional distress damages against Equifax for improper handling of personal identifying information. *See Drew v. Equifax Info. Servs., LLC*, No. C 07-00726 SI, 2010 WL 5022466, at *3 (N.D. Cal. Dec. 3, 2010). The Fourth Circuit has upheld a jury verdict of $245,000 for mental anguish for a victim of "systemic manipulation of her personal information" based in part on comparison to jury verdicts for emotional distress damages in defamation cases, which the court placed generally "in the range of $250,000." *Sloane v. Equifax Information Services, LLC*, 510 F. 3d 495, 505-06 (4th Cir. 2007).

* * *

A California district court has granted a plaintiff $700,000 in punitive damages for improper handling of personal identifying information. *See Drew v. Equifax Info. Servs., LLC*, No. C 07-00726 SI, 2010 WL 5022466, at *3 (N.D. Cal. Dec. 3, 2010). The United States Supreme Court has stated that damage awards at a ratio of 9:1 between punitive damages and actual damages are permissible. *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 425 (2003). The Ninth Circuit has even upheld awards at a ratio of 300,000:1 under certain circumstances. *Arizona v. ASARCO LLC*, 773 F.3d 1050, 1061 (9th Cir. 2014) (en banc).

VIII. DERIVATIVE AND DEMAND-MADE ALLEGATIONS

271. Plaintiff brings this action derivatively, in the right and for the benefit of Equifax, to redress injuries suffered, and to be suffered, by Equifax as a direct result of the breaches of fiduciary duties, unjust enrichment, insider selling, violation of Section 14(a) of the Exchange Act, issuing false and misleading statements in

violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5 promulgated thereunder, violations of Section 29(b) of the Exchange Act, corporate waste, and contribution and indemnification by the Individual Defendants. Equifax is named as a nominal defendant solely in a derivative capacity.

272. Plaintiff will adequately and fairly represent the interests of Equifax in enforcing and prosecuting its rights, and has hired counsel experienced in shareholder derivative litigation.

273. Plaintiff is, and has continuously been, a shareholder of Equifax since 2005, including at the time of the Individual Defendants' wrongdoing complained of herein.

274. At all times relevant hereto, each of the Individual Defendants was the agent of each of the other Individual Defendants and of Equifax, and was at all times acting within the course and scope of such agency.

275. Each Individual Defendant, by virtue of his or her position as a director and/or officer, owes, and owed, to Equifax and its shareholders the fiduciary duties of loyalty and good faith, and the exercise of due care and diligence in the management and administration of the affairs of Equifax, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations

as directors and officers of Equifax, the absence of good faith on his or her part, and a reckless disregard for their duties to Equifax and its shareholders that the Individual Defendants were aware or should have been aware posed a risk of serious injury to Equifax.

276. The Individual Defendants each breached their duties of loyalty and good faith by allowing the other Individual Defendants to cause, or by themselves causing, the Company to operate in evident violation of law and to issue false and/or misleading statements that misled shareholders into believing that disclosures related to the Company's business practices, operations, financials, compliance policies and practices, and internal controls were truthful and accurate when made.

277. Equifax is controlled by its Board, which currently consists of 11 directors. Ten of the current directors are named as Defendants in this action: Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton. Non-Defendant Scott A. McGregor ("McGregor") was added to the Equifax Board on October 26, 2017.

278. The Director Defendants were directors throughout the Relevant Period, and, as such, had a fiduciary duty to ensure that the Company operated in a lawful manner and to ensure that Company management had identified and developed processes to mitigate risks facing the organization, including risks arising

from data theft and the loss of critically sensitive consumer information. Despite red flags indicating deficient data security, the Board failed to ensure that Company management had identified and developed processes to mitigate risks facing the organization, including risks arising from data theft and the loss of critically sensitive consumer information.

279. Specifically, despite learning that its data security systems were not legally compliant, the Individual Defendants consciously failed to: (i) develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) develop, implement, and maintain proper data security systems, controls, and monitoring systems; (iv) develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) adequately assess the risks associated with the Company's data security; (vi) adequately assess the risks associated with the Company's executive compensation plan; (vii) maintain adequate corporate accounting and corporate financial-reporting resources; (viii) adequately assess the risks associated with the Company's financial reporting; and (ix) maintain effective internal controls over financial reporting.

280. The Director Defendants also had fiduciary duties to ensure that its SEC filings, press releases, and other public statements and presentations on behalf of the Company concerning its financial and business prospects were accurate.

281. Indeed, each of the Director Defendants signed the improper 2016 10-K. The 2016 10-K was improper because, *inter alia*, it misrepresented and/or failed to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by the harm they caused the Company; (vii) the Company had inadequate corporate accounting and corporate financial-reporting resources; (viii) the Company inadequately assessed the risks

associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial reporting; and (x) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times. As a result, the Director Defendants each face a substantial likelihood of liability for their breaches of fiduciary duties, and are incapable of considering Plaintiff's Demand.

282. Moreover, the Director Defendants, as Company directors (and, in the case of Director Defendants Daleo, Hough, McKinley, and Templeton, also as Audit Committee Defendants), owed a duty to, in good faith and with due diligence, exercise reasonable inquiry, oversight, and supervision to ensure that the Company's internal controls and/or internal auditing and accounting controls over financial reporting were sufficiently robust and effective (and/or were being implemented effectively), and to ensure that the Audit Committee's duties were being discharged in good faith and with the required diligence and due care. Instead, they knowingly and/or with reckless disregard reviewed, authorized, and/or caused the publication of materially false and misleading statements throughout the Relevant Period that caused the Company's stock to trade at artificially-inflated prices.

283. The Individual Defendants also violated, or failed to prevent others from violating, *inter alia*, federal securities laws (which have resulted in, and exposed the Company to, the Securities Class Actions), as well as myriad federal, state, and/or municipal laws, rules, and regulations governing data breach, credit reporting, consumer protection, business and/or trade practices, privacy, and/or torts (which have resulted in, and exposed the Company to, the Consumer Class Actions and the Consumer Protection Actions). As a result of these and other breaches of fiduciary duties and violations of law, Equifax has expended, and will continue to expend, significant sums of money to rectify the Individual Defendants' wrongdoing.

284. Thus, the Individual Defendants, because of their positions of control and authority as directors and/or officers of Equifax, were able to, and did, directly, and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by the Company, which resulted in substantial harm to Equifax.

285. Specifically, as members of the Audit Committee, Defendants Daleo (Chair), Hough, McKinley, and Templeton breached their fiduciary duties of good faith and loyalty by, *inter alia*, failing to (i) implement sufficient internal controls and procedures, and/or recklessly and indifferently failing to follow internal controls

and procedures, to ensure the accuracy of the Company's public statements; (ii) implement, and ensure that the Company maintained, adequate corporate accounting and corporate financial-reporting resources; (iii) adequately assess the risks associated with the Company's financial reporting; and (iv) implement sufficient systems for complying with legal and regulatory requirements and/or recklessly and indifferently failing to follow such systems. Because of these failures, the Company operated in evident violation of law, and issued false and misleading statements concerning the Company's business practices, operations, financials, compliance policies and practices, and internal controls, as alleged herein.

286. Additionally, as members of the Technology Committee, Defendants Feidler, Hough (Chair), McKinley, Stock, and Templeton breached their fiduciary duties of good faith and loyalty by, *inter alia*, failing to (i) develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) develop, implement, and maintain proper data security systems and controls; (iv) develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; and (v) adequately assess the risks with the Company's data security. Because of these failures, the Company operated in evident violation of the law, and issued false and

misleading statements concerning the Company's business practices, operations, financials, compliance policies and practices, and internal controls, as alleged herein.

287. Finally, as members of the Compensation Committee, Defendants Daleo, Humann, Marcus (Chair), and Marshall breached their fiduciary duties of good faith and loyalty by, *inter alia*, failing to monitor, and assess the risk associated with, the Company's executive compensation plan and failed to create a compensation system whereby management is held accountable for its improper and/or illegal actions. Because of this failure, the Company issued false and misleading statements concerning the Company's business practices, operations, financials, compliance policies and practices, and internal controls, as alleged herein.

288. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct and have acted in concert with, and conspired with, one another in furtherance of their wrongdoing. The Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

289. During all times relevant hereto, the Individual Defendants collectively and individually initiated a course of conduct that was designed to mislead shareholders into believing that the Company had effective compliance policies and procedures and internal controls, that it was operating its business in compliance

with the law, and that its financials were better than they actually were. In furtherance of this plan, conspiracy, and course of conduct, the Individual Defendants collectively and individually took the actions set forth herein.

290. The purpose and effect of the Individual Defendants' conspiracy, common enterprise, and/or common course of conduct was, among other things, to: (a) disguise the Individual Defendants' violations of law, including breaches of fiduciary duties, insider selling, corporate waste, and unjust enrichment; and (b) disguise and misrepresent the Company's unlawful business practices and operations, lack and/or failure of compliance policies and practices, artificially-inflated financials and stock price, and faulty internal controls.

291. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by causing the Company to operate in evident violation of, *inter alia*, myriad federal, state, and municipal laws, rules, and regulations, as well as to purposefully, recklessly, or negligently release false and misleading statements. Because the actions described herein occurred under the authority of the Board, each of the Individual Defendants was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

292. Each of the Individual Defendants aided and abetted, and rendered substantial assistance in, the wrongs complained of herein. In taking such actions to substantially assist the commissions of the wrongdoing complained of herein, each Individual Defendant acted with knowledge of the primary wrongdoing, substantially assisted the accomplishment of that wrongdoing, and was aware of his or her overall contribution to and furtherance of the wrongdoing.

293. Before filing this derivative action, Plaintiff first demanded that the Board take action to investigate and redress the misconduct alleged herein.

294. Specifically, on September 11, 2017, in accordance with O.C.G.A. § 14-2-742, Plaintiff sent the Demand to the Board to take action to remedy the harm to Equifax caused by certain of the Company's officers and directors who violated and caused the Company to violate the federal securities laws and Georgia law, and who accordingly caused the damages and harms the Company has suffered in connection with the events detailed herein, including those events underlying the Securities Class Actions, the Consumer Class Actions, and the Consumer Protection Actions. A true and correct copy of the Demand is attached hereto as **Exhibit A**.

295. On October 6, 2017, the Company sent a letter in respond to the Demand requesting documentation confirming Plaintiff's status as a current and

continuous holder of Equifax stock since 2005. A true and correct copy of the Company's October 6, 2017 letter is attached hereto as **Exhibit B**.

296. On October 11, 2017, counsel for Plaintiff sent a letter responding to the Company's October 6, 2017 letter. Plaintiff's October 11, 2017 letter noted that although the Company failed to cite any law to support such a request, counsel for Plaintiff would be willing to provide documentation evidencing Plaintiff's status as a current and continuous shareholder of Equifax since 2005 once the Company confirmed that the information would be designated "Attorneys' Eyes Only" and treated as highly confidential. A true and correct copy of counsel for Plaintiff's October 11, 2017 letter is attached hereto as **Exhibit C**.

297. On October 23, 2017, without providing explanation or rationale, the Company refused to designate Plaintiff's ownership information "Attorneys' Eyes Only" and highly confidential. A true and correct copy of the Company's October 23, 2017 letter is attached hereto as **Exhibit D**.

298. On October 26, 2017, the Company announced that Non-Defendant McGregor had been added to the Board and that he would serve on the Technology Committee.

299. On October 30, 2017, counsel for the Plaintiff sent the Company a letter in response to the Company's October 6, 2017 letter. Rather than belabor the

confidentiality of Plaintiff's ownership information, counsel for Plaintiff provided the Company with a redacted brokerage statement evidencing Plaintiff's continuous ownership of Equifax since February 1, 2005. A true and correct copy of counsel for Plaintiff's October 30, 2017 letter is attached hereto as **Exhibit E**.

300. On November 27, 2017, the Board caused the Company to send, through its counsel, Wilmer Cutler Pickering Hale and Dorr LLP ("Wilmer Hale"), a letter to counsel for Plaintiff that stated, *inter alia*, that (i) the Board formed a Demand Review Committee (the "Committee") of the Board in response to the Demand; (ii) the Committee consists of purportedly "independent"[53] Director Defendants Stock, Hough, and Non-Defendant McGregor; (iii) the Committee "is undertaking a thorough investigation of all allegations contained in the Demand"; and (iv) the Committee will contact counsel for Plaintiff "when the investigation is complete." A true and correct copy of counsel for the Company's November 27, 2017 letter is attached hereto as **Exhibit F**. The letter does not explain why, despite (i) having months to investigate the wrongdoing described in the Demand, and (ii) the Company announcing on September 7, 2017, that "the Company's investigation is substantially complete," the Company has yet to take suitable legal

[53] Hough and Stock served on the Board's Technology Committee, and Stock was also on the Board's Audit Committee, and therefore had heightened duties and responsibilities in connection with the Data Breach. *See* §§ IV.D.5.a–b, *supra*.

action against any officer or director of the Company found to have committed or participated in the wrongdoing described in the Demand.

301. On November 29, 2017, counsel for Plaintiff responded to the Company's November 27, 2017 letter. Plaintiff's November 29, 2017 letter to Wilmer Hale acknowledged receipt of the Company's November 27, 2017 letter and requested the following information from the Company so that Plaintiff could continue his proactive protection of the interests of Equifax: (i) the date on which the Committee was commissioned to undertake its investigation of the Demand; (ii) an explanation as to how each member of the Committee was selected and determined to be disinterested and independent; (iii) details regarding the scope of the Committee's mandate; (iv) details regarding the authority of the Committee to take action regarding the matters identified in the Demand; and (v) details regarding Wilmer Hale's involvement, including when the firm was retained to advise the Committee and whether, how, and by whom the firm was determined to be independent. Counsel for Plaintiff also requested an opportunity for the Committee to brief counsel for Plaintiff regarding the current status of the investigation, what remains to be done to complete the evaluation, the work plan for doing so, and the expected timeframe by which the Committee anticipates completing its work. A

true and correct copy of counsel for Plaintiff's November 29, 2017 letter is attached hereto as **Exhibit G**.

302. As of the time of the filing of this Complaint, the Company has not responded to Plaintiff's November 29, 2017 letter.

303. As ninety days have expired from the date the Demand was made, Plaintiff rightfully files this shareholder derivative action, and this Complaint, on behalf of the Company.

IX. CAUSES OF ACTION

COUNT I
Breach of Fiduciary Duty
(Against All Individual Defendants)

304. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

305. Each of the Defendants owed and owe fiduciary duties to Equifax and its shareholders. By reason of their fiduciary relationships, Defendants specifically owed and owe Equifax the highest obligation of good faith, fair dealing, loyalty, and due care in the administration and management of the affairs of the Company, including the Company's financial reporting, internal controls, and compensation practices. These duties include the duty of full and fair disclosure to shareholders, also known as the duty of candor. To execute this duty, the Individual Defendants

were required to disseminate accurate, truthful, and complete information to shareholders at all times.

306. Each of the Defendants each knowingly, recklessly, or negligently: (i) caused the Company to maintain inadequate data security measures, resulting in the Company operating in evident violation of the law; (ii) made or caused to be made false and misleading statements that misrepresented or failed to disclose material information concerning the Company; (iii) approved the issuance of such false and/or misleading statements; (iv) failed to take actions to correct such false and/or misleading statements after they had been disseminated by the Company; and (v) failed to address the misconduct alleged herein. These actions were not a good faith exercise of prudent business judgment to protect and promote the Company's corporate interests, and thereby each such Defendant consciously and deliberately breached his or her fiduciary duties of candor, good faith, loyalty, and reasonable inquiry to Equifax and its shareholders in at least the following specific ways:

a. overseeing and endorsing the grossly deficient data security that allowed the Data Breach to occur;

b. failing to comply with industry standards for the safekeeping and maintenance of the personal and financial information, including allowing the Company's employees to store critically sensitive PII data in online portals in

unencrypted and unredacted plaintext, or other methods that would have rendered the PII unusable, thus causing the Data Breach;

c. failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect personal and financial information, including allowing the Company's employees to fail to remedy a critical software remedy despite a March 8, 2017 alert from U.S.-CERT warning Equifax of the dire need to do so, and despite knowledge of a 2016 Deloitte security audit of Equifax's data security that specifically identified Equifax's careless approach to patching systems, thus causing the Data Breach;

d. willfully ignored or consciously disregarded the obvious and pervasive problems with Equifax's internal control and compliance practices and procedures, and other red flags related to the Company's grossly deficient data security, and consciously failed to make a good faith effort to correct the problems or their recurrence.

e. failing to timely disclose the Data Breach to investors, consumers, and appropriate regulators manner when they reasonably believed that PII was acquired by unauthorized persons, or when they were aware of a

breach of Equifax's security system (which was reasonably likely to result in misuse of Delaware residents' personal information);

f. forcing victims of the Data Breach to sign up for arbitration and other terms and conditions in order to exculpate themselves from the Data Breach;

g. structuring the Company's compensation policies so that Company employees were incentivized to maintain lax data security, and rewarding Company executives for the purported "success" of driving consumers to sign up for Equifax's credit monitoring and credit locking services while immunizing such executives from the negative ramifications of legal consequences the Company may face as a result of their actions or inaction;

h. allowing Equifax insiders to conduct insider sales and dispositions of Company stock while in the possession of material, adverse, and non-public information;

i. approving the Company's repurchase of Equifax shares at artificially inflated prices;

j. allowing Equifax's public statements on data security to be false and misleading, which also resulted in the artificial inflation of the Company's share price;

k. allowing for inadequate risk controls over the Company's policies and practices, which allowed the Data Breach, yet immunizing certain executives from financial fallout due to such policies and practices as a result of a flawed executive compensation plan as detailed herein; and

l. engaging in abuse of control and gross mismanagement of Equifax's assets and business through a failure to prevent the Data Breach.

307. In direct violation of their fiduciary duties, the Individual Defendants each knowingly or recklessly issued, or approved the issuance of, false and misleading public statements to shareholders that misrepresented and/or failed to disclose material information concerning the Company's business model, future business and financial prospects, business practices, compliance policies and practices, and internal controls. Specifically, the Individual Defendants made, or caused the Company to make, false and misleading statements, and/or failed to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security

breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by the harm they caused the Company; (vii) the Company had inadequate corporate accounting and corporate financial reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial reporting; and (x) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times. These actions could not have been a good faith exercise of prudent business judgment to protect and promote the best interests of the Company and its shareholders.

308. Defendants, individually and in concert, engaged in the above referenced conduct in intentional, reckless, or grossly negligent breaches of the fiduciary duties they owed to Equifax to protect its rights and interests.

309. Defendants had actual or constructive knowledge that they had caused the Company to improperly misrepresent its financial condition, and they failed to correct the Company's public statements. Defendants had actual knowledge of the misstatements and omissions of material facts set forth in this Complaint, or acted with reckless disregard for the truth, in that they failed to ascertain and disclose such facts, even though such facts were available to them. Such material misrepresentations and omissions were committed knowingly or recklessly, and for the purpose and effect of artificially inflating the price of Equifax's securities.

310. These actions were taken in bad faith, and were not a good-faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

311. Additionally, the Individual Defendants have specific fiduciary duties as defined by the Company's corporate governance documents, including the Code and the charters of various Board committees that, had they been discharged in accordance with Defendants' obligations, would have necessarily prevented the misconduct and the consequent harm to the Company alleged in this Complaint.

312. Defendants conspired to abuse, and did abuse, the control vested in them by virtue of their positions in the Company.

313. As a direct and proximate result of Defendants' breaches of their fiduciary obligations, Equifax has sustained, and continues to sustain, significant damages. As a result of the misconduct alleged in this Complaint, Defendants are liable to the Company.

COUNT II
Unjust Enrichment
(Against All Individual Defendants)

314. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

315. During the Relevant Period, Defendants received bonuses, stock options, stock, or similar compensation from Equifax that was tied to the Company's financial performance, or otherwise received compensation that was unjust in light of Defendants' bad faith conduct, violation of the Company's Code and other charters, and self-dealing.

316. In addition, the Insider Trading Defendants' sales provided a personal benefit to those Defendants not shared equally by the Company's other shareholders, and the Insider Trading Defendants should be required to return their profits to the Company and its shareholders.

317. Plaintiff, as shareholder and representative of Equifax, seeks restitution from Defendants and seeks an order of this Court disgorging all profits, benefits, and other compensation—including any salary, options, performance-based compensation, and stock—obtained by the Individual Defendants due to their wrongful conduct alleged in this Complaint.

COUNT III
Breach of Fiduciary Duty for
Insider Selling and Misappropriation of Information
(Against the Insider Selling Defendants)

318. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

319. At the time of the stock sales set forth in ¶¶233–246 above, the Insider Selling Defendants knew or recklessly disregarded the information described in this Complaint regarding the Equifax's lax data security and/or the Data Breach and sold Equifax common stock on the basis of that information.

320. The material, adverse, and non-public information at-issue—which concerned Equifax's business practices, operations, financials, compliance policies and practices, and the sufficiency of its internal controls, as described in greater detail herein above—was a proprietary asset belonging to the Company that must be used to benefit the Company and all its shareholders on equal terms. Instead, the

Insider Selling Defendants misappropriated this information entirely for their own benefit.

321. At the time of their stock sales, the Insider Selling Defendants either knew the truth about the Data Breach—which at that time, and for over a month thereafter, they and the other Individual Defendants knowingly and intentionally withheld from the public—or the truth about the Company's falsely and/or misleadingly reported business practices and operations, lack and/or failure of compliance policies and practices, artificially-inflated financials and stock price, and faulty internal controls.

322. The Insider Selling Defendants' sales of stock while in possession and control of this material, adverse, and non-public information was a breach of their fiduciary duties of loyalty and good faith.

323. Since the use of the Company's proprietary information for their own gain constitutes a breach of the Insider Selling Defendants' fiduciary duties, the Company is entitled to the imposition of a constructive trust on any profits the Insider Selling Defendants obtained thereby.

COUNT IV
Violation of Section 14(a) of the Exchange Act and SEC Rule 14a-9
(Against the Director Defendants)

324. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein, except to the extent those allegations plead knowing or reckless conduct by the Director Defendants. This claim is based solely on negligence, not on any allegation of reckless or knowing conduct by, or on behalf of, the Director Defendants. Plaintiff specifically disclaims any allegations of, reliance upon any allegation of, or reference to any allegation of fraud, scienter, or recklessness with regard to this claim.

325. SEC Rule 14a-9 (17 C.F.R. § 240.14a-9), promulgated under Section 14(a) of the Exchange Act, provides:

> No solicitation subject to this regulation shall be made by means of any proxy statement form of proxy, notice of meeting or other communication, written or oral, containing any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading or necessary to correct any statement in any earlier communication with respect to the solicitation of a proxy for the same meeting or subject matter which has become false or misleading.

326. The Director Defendants negligently issued, caused to be issued, and participated in the issuance of materially misleading written statements to shareholders that were contained in the 2017 Proxy Statement. The 2017 Proxy

Statement contained proposals to Equifax's shareholders urging them to re-elect the members of the Board and approve executive compensation. The 2017 Proxy Statement, however, misstated or failed to disclose (i) deficiencies in Equifax's internal and disclosure controls that were known to the Board when the 2017 Proxy Statement was filed; (ii) reporting failures known to the Board when the 2017 Proxy Statement was filed, which failed to address known data security vulnerabilities of Equifax; (iii) Equifax's inadequate controls that were known to the Board when the 2017 Proxy Statement was filed; (iv) Board-approved compensation structures that encouraged data security vulnerabilities to exist; (v) the fact that Equifax employed deficient data security even after the Board learned of specific and critical data security vulnerabilities, and (vi) that Equifax faced significant reputational harm when the truth would inevitably unfold. By reasons of the conduct alleged in this Complaint, the Director Defendants violated Section 14(a) of the Exchange Act and SEC Rule 14a-9, promulgated thereunder.

327. The 2017 Proxy Statement violated Section 14(a) and Rule 14a-9 by misrepresenting or failing to disclose that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop,

implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by the harm they caused the Company; (vii) the Company had inadequate corporate accounting and corporate financial-reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal controls over financial reporting; and (x) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times.

328. The false and/or misleading statements in the 2017 Proxy Statement were the essential link to the directors' reelection. Equifax shareholders voted for the 2017 Proxy Statement because of its false and/or misleading statements, and the losses to the Company resulted directly from the 2017 Proxy Statement vote—if the

Individual Defendants elected to the Board as a result of the 2017 Proxy Statement had not been elected to the Board, the Data Breach would likely not have occurred because security measures would likely have been enacted and the compensation plan immunizing certain executives from the legal fallout of the Data Breach would not have been approved.

329. Plaintiff, on behalf of Equifax, thereby seeks relief for damages inflicted upon the Company based on the misleading 2017 Proxy Statement in connection with the improper re-election of the members of the Board and approval of executive compensation.

330. This action was timely commenced within three years of the date of the 2017 Proxy Statement and within one year from the time Plaintiff discovered, or reasonably could have discovered, the facts on which this claim is based.

COUNT V
Violations of Section 10(b) of the Exchange Act and SEC Rule 10b-5 Promulgated Thereunder (Against Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton)

331. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

332. During the Relevant Period, in connection with Equifax's repurchases of Equifax shares, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton disseminated or

approved false or misleading statements about Equifax specified in ¶¶218–231, which they knew, or recklessly disregarded, were false or misleading and were intended to deceive, manipulate, or defraud. Those false or misleading statements and Defendants' course of conduct were designed to artificially-inflate the price of the Company's common stock.

333. At the same time that the price of the Company's common stock was inflated due to the false or misleading statements made by Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, these Defendants caused the Company to repurchase millions of shares of its own common stock at prices that were artificially inflated due to these Defendants' false or misleading statements. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton engaged in a scheme to defraud Equifax by causing the Company to spend at least $77 million purchasing shares of Equifax stock at artificially-inflated prices.

334. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton violated Section 10(b) of the Exchange Act and SEC Rule 10b-5 in that they (a) employed devices, schemes, and artifices to defraud; (b) made untrue statements of material facts or omitted to state

material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices, and a course of business that operated as a fraud or deceit upon Equifax in connection with the Company's purchases of Equifax stock during the Relevant Period.

335. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, individually and in concert, directly and indirectly, by the use of means or instrumentalities of interstate commerce or of the United States mails, engaged and participated in a continuous course of conduct that operated as a fraud and deceit upon the Company; made various false or misleading statements of material facts and omitted material facts necessary in order to make the statements, in light of the circumstances under which they were made, not misleading; made the above statements intentionally or with a severely reckless disregard for the truth; and employed devices and artifices to defraud in connection with the purchase and sale of Equifax stock, which were intended to, and did, (i) deceive Equifax regarding, among other things, its grossly deficient data security, the Company's internal controls and compensation practices, and the Company's financial statements; (ii) artificially inflate and maintain the market price of Equifax stock; and (iii) cause Equifax to purchase the Company's

stock at artificially-inflated prices, and suffer losses when the true facts became known. At the time the statements alleged herein in ¶¶218–231 were made, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton were in possession of the material, adverse, non-public information that: (i) the Company failed to develop, implement, and maintain adequate measures to safeguard and protect its data systems; (ii) the Company failed to develop, implement, and maintain adequate monitoring systems to detect security breaches; (iii) the Company failed to develop, implement, and maintain proper data security systems, controls, and monitoring systems in place; (iv) the Company failed to develop, implement, and maintain adequate measures to respond to known risks concerning its data security systems, controls, and monitoring systems; (v) the Company inadequately assessed the risks associated with the Company's data security; (vi) the Company inadequately assessed the risks associated with the Company's executive compensation plan, and inadequately explained that the executive compensation plan actually served to protect certain executives from financial ramifications to the Company caused by harm they caused the Company; (vii) the Company had inadequate corporate financial-reporting resources; (viii) the Company inadequately assessed the risks associated with the Company's financial reporting; (ix) Equifax failed to maintain effective internal

controls over financial reporting; (x) the Company was recklessly relying on a single employee to address US-CERT warnings regarding critical data security systems; (xi) the Company had been warned by Deloitte in 2016 that Equifax was taking a careless approach to patching critical data security systems; (xii) Mandiant, in March or April 2017, had warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems; (xiii) the Company lacked a plan to quickly, effectively, and sufficiently respond to a major data breach; and (xiv) as a result of the foregoing, Equifax's public statements, made or caused to be made by the Individual Defendants, were materially false and misleading and/or lacked a reasonable basis at all relevant times.

336. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton were among the senior management and the directors of the Company, and were, therefore, directly responsible, and are liable for all materially false or misleading statements made during the Relevant Period, as alleged above.

337. As described above, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton acted with scienter throughout the Relevant Period, in that they acted either with intent to deceive, manipulate, or defraud, or with severe recklessness. The misstatements and

omissions of material facts set forth in this Complaint were either known to Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton or were so obvious that these Defendants should have been aware of them. Throughout the Relevant Period, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton also had a duty to disclose new information that came to their attention and rendered their prior statements to the market materially false or misleading.

338. The false or misleading statements of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton were made in connection with the purchase or sale of the Company's stock, both by the Company itself and by the Insider Selling Defendants.

339. As a result of the misconduct alleged herein of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, Equifax has, and will continue to, suffer damages in that it paid artificially-inflated prices for Equifax common stock purchased as part of the repurchase program and suffered losses when the previously undisclosed facts relating to Equifax's lax data security were disclosed beginning in September 2017. Equifax would not have purchased these securities at the prices it paid, or at all, but

for the artificial inflation in the Company's stock price caused by the false or misleading statements of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton.

340. As a direct and proximate result of the wrongful conduct of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, the Company suffered damages in connection with its purchases of Equifax stock during the Relevant Period. By reason of such conduct, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton are liable to the Company pursuant to Section 10(b) of the Exchange Act and SEC Rule 10b-5.

341. Plaintiff brought this claim within two years of their discovery of the facts constituting the violation and within five years of the violation.

COUNT VI
Violations of Section 29(b) of the Exchange Act
(Against Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton)

342. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

343. As a result a result of their conduct, as alleged in this Complaint, Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton violated Sections 10(b) and 14(a) of the

Exchange Act during the time they entered into contracts with Equifax regarding their compensation.

344. If Equifax attempts to recover compensation from Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, these Defendants might assert a breach of contract claim and/or seek severance.

345. Section 29(b) of the Exchange Act provides equitable remedies that include, among other things, provisions allowing for the voiding of contracts where the performance of the contract involved violation of any provision of the Exchange Act.

346. Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton violated provisions of the Exchange Act while performing their duties arising under various employment and other contracts they entered into with Equifax.

347. Equifax was, and is, an innocent party with respect to the Exchange Act violations of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton.

348. Plaintiff, on behalf of Equifax, seeks rescission of the contracts between Equifax and Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann,

Marcus, Marshall, McKinley, Stock, and Templeton due to these Defendants' violations of the Exchange Act while performing their job duties.

349. Even if the contracts are not rescinded by the Court as a result of the Exchange Act violations of Defendants Smith, Gamble, Daleo, Driver, Feidler, Hough, Humann, Marcus, Marshall, McKinley, Stock, and Templeton, the Court can, and should, award equitable remedies in the form of injunctive relief barring these Defendants from asserting breach of contract by Equifax in any action by Plaintiff on behalf of Equifax to return compensation from these Defendants.

350. Plaintiff seeks only declaratory, injunctive, and equitable relief in this claim.

COUNT VII
Corporate Waste
(Against the Director Defendants)

351. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

352. The Director Defendants have a fiduciary duty to protect Equifax's assets from loss or waste.

353. By approving the stock repurchase program, the Director Defendants breached this fiduciary duty and have caused Equifax to waste its corporate assets on the repurchase of stock at artificially-inflated prices.

354. In addition, the Director Defendants caused Equifax to waste its corporate assets by allowing Smith to "retire" as CEO and director, Susan Mauldin to "retire" as the Company's CSO, and David C. Webb to "retire" as the Company's CIO, even though Equifax had grounds to terminate Smith, Mauldin, and Webb for cause.

355. As a result of the Director Defendants' corporate waste, the Company has suffered damages.

COUNT VIII
Contribution and Indemnification
(Against All Individual Defendants)

356. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

357. This claim is brought derivatively on behalf of the Company against the Individual Defendants for contribution and indemnification.

358. Equifax is named as a defendant in the Securities Class Actions filed in this District, asserting claims under the federal securities laws for, *inter alia*, false and misleading statements. In the event the Company is found liable for violating the federal securities laws, the Company's liability will arise, in whole or in part, from the intentional, knowing, or reckless acts or omissions of some or all of the Individual Defendants as alleged herein. The Company is entitled to receive

contribution from those Individual Defendants in connection with the Securities Class Actions against the Company currently pending in this District.

359. Accordingly, Equifax is entitled to all appropriate contribution or indemnification from the Individual Defendants.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

A. Declaring that Defendants have breached their fiduciary duties to Equifax;

B. Against all Defendants for the amount of damages sustained by the Company as a result of the violations set forth above from each Defendant, jointly and severally, together with prejudgment and post-judgment interest thereon;

C. Directing Equifax to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect Equifax and its shareholders from a repeat of the damaging events described herein, including but not limited to putting forward for shareholder vote resolutions for amendments to the Company's By-Laws or Articles of Incorporation, and taking such other action as may be necessary to place before shareholders for a vote the following corporate governance proposals or policies:

- a proposal to require the Board to periodically review the Company's potential cybersecurity exposure and policies, including the creation of a Board committee who specific role it is to monitor and oversee such exposure and policies;

- a proposal to require the Board to develop an action plan to respond to a breach in consumer data, including employee and Board responsibilities, who should be contacted and when, how the Company will communicate to the public, and how the breach will be assessed;

- a proposal to implement additional safeguards to protect sensitive consumer data, including a review of who has access to critical data, and develop policies around how this information is documented, stored, accessed, and shared within the Company;

- a proposal to strengthen the Board's supervision of operations and compliance with applicable state and federal laws and regulations;

- a proposal to strengthen the Company's internal reporting and financial disclosure controls;

- a proposal to develop and implement procedures for greater shareholder input into the policies and guidelines of the Board;

- a proposal to modify executive compensation policies to align the interests of executives with the interests of the Company, incentivize executives ensure the Company's compliance with all applicable laws, and ensure that executives' compensation is impacted by the Company's legal expenses;

- a proposal to ensure the accuracy of the qualifications of Equifax's directors, executives, and other employees;

- a proposal to require an independent Chairman of the Board;

- a provision to permit the shareholders of Equifax to nominate at least four candidates for election to the Board to replace existing directors;

- a proposal to strengthen the Company's procedures for the receipt, retention, and treatment of complaints received by the Company regarding internal controls; and
- a provision to appropriately test and then strengthen the Company's internal operational control functions;

D. Ordering an accounting of all compensation awarded to the Individual Defendants during the Relevant Period;

E. Granting extraordinary equitable or injunctive relief as permitted by law or equity, including attaching, impounding, imposing a constructive trust on, or otherwise restricting Defendants' assets so as to assure that Plaintiff, on behalf of Equifax, has an effective remedy;

F. Awarding to Equifax restitution from the Individual Defendants, and ordering disgorgement of all profits, benefits, and other compensation obtained by the Individual Defendants;

G. Canceling the votes to re-elect the Director Defendants in connection with the annual shareholder meetings in 2017, and ordering Defendants to disgorge to the Company all compensation they received for service on the Board following those invalid elections;

H. Awarding to Plaintiff the costs and disbursements of this action, including reasonable attorneys' fees, accountants' and experts' fees, costs, and expenses; and

I. Granting such other and further relief as the Court deems just and proper.

XI. JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 22, 2018

JOHNSON FISTEL, LLP

By: *s/ Michael I. Fistel*
MICHAEL I. FISTEL, JR.
(Ga. Bar No. 262062)

William W. Stone (Ga. Bar No. 273907)
David A. Weisz (Ga. Bar No. 134527)
Murray House
40 Powder Springs Street
Marietta, GA 30064
Telephone: (770) 200-3104
Facsimile: (770) 200-3101
michaelf@johnsonfistel.com
williams@johnsonfistel.com
davidw@johnsonfistel.com

Attorneys for Plaintiff Bax

VERIFICATION

I, Robert L. Bax, verify that I have reviewed the foregoing Verified Shareholder Derivative Complaint, and that the allegations as to me are true and correct and that the other allegations upon information and belief are true and correct.

Dated: January 22, 2018

DocuSigned by:
F7BA741DFCA7423...

(Signature of Robert L. Bax)